Secrecy Capacity Region of a Multi-Antenna Gaussian Broadcast Channel with Confidential Messages

Ruoheng Liu and H. Vincent Poor

Abstract

In wireless data networks, communication is particularly susceptible to eavesdropping due to its broadcast nature. Security and privacy systems have become critical for wireless providers and enterprise networks. This paper considers the problem of secret communication over the Gaussian broadcast channel, where a multi-antenna transmitter sends independent confidential messages to two users with *information-theoretic secrecy*. That is, each user would like to obtain its own confidential message in a reliable and safe manner. This communication model is referred to as the multi-antenna Gaussian broadcast channel with confidential messages (MGBC-CM). Under this communication scenario, a secret dirty-paper coding scheme and the corresponding achievable secrecy rate region are first developed based on Gaussian codebooks. Next, a computable Sato-type outer bound on the secrecy capacity region is provided for the MGBC-CM. Furthermore, the Sato-type outer bound prove to be consistent with the boundary of the secret dirty-paper coding achievable rate region, and hence, the secrecy capacity region of the MGBC-CM is established. Finally, two numerical examples demonstrate that both users can achieve positive rates simultaneously under the information-theoretic secrecy requirement.

Index Terms

secret communication, broadcast channels, multiple antennas, information-theoretic secrecy

I. Introduction

The need for efficient, reliable, and secret data communication over wireless networks has been rising rapidly for decades. Due to its broadcast nature, wireless communication is particularly susceptible to eavesdropping. The inherent problematic nature of wireless networks exposes not only the risks and vulnerabilities that a malicious user can exploit and severely compromise the network, but also multiplies information confidentiality concerns with respect to in-network terminals. Hence, security and privacy systems have become critical for wireless providers and enterprise networks.

This research was supported by the National Science Foundation under Grants ANI-03-38807 and CNS-06-25637. The material in this paper was presented in part at the First International Workshop on Information Theory for Sensor Networks, Santa Fe, NM, June 18 - 20, 2007

Ruoheng Liu and H. Vincent Poor are with Department of Electrical Engineering, Princeton University, Princeton, NJ 08544, USA, email: {rliu,poor}@princeton.edu.

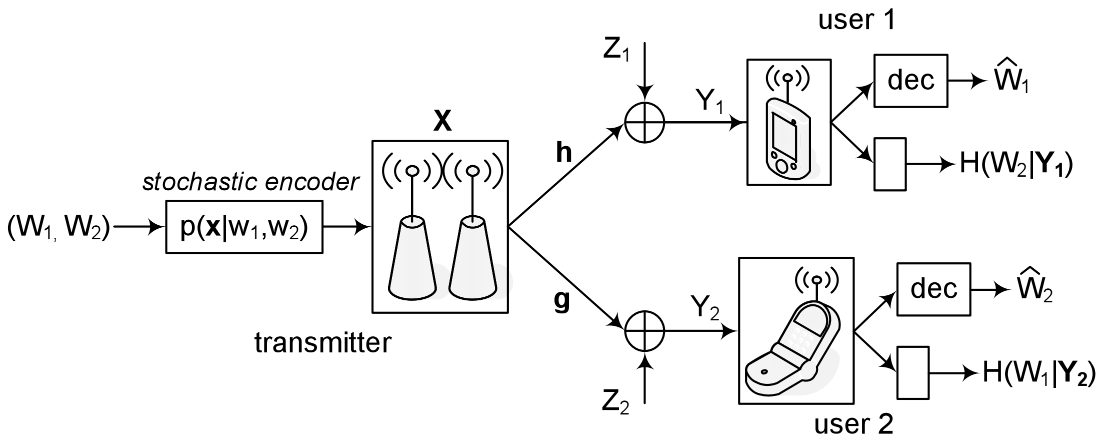

Fig. 1. Multiple-antenna Gaussian broadcast channel with confidential message

In this work, we consider multiple antenna secret broadcast in wireless networks. This research is inspired by the seminal paper [1], in which Wyner introduced the so-called *wiretap channel* and proposed an information theoretic approach to secret communication schemes. Under the assumption that the channel to the eavesdropper is a degraded version of that to the desired receiver, Wyner characterized the capacity-secrecy tradeoff for the discrete memoryless wiretap channel and showed that secret communication is possible without sharing a secret key. Later, the result was extended by Csiszár and Körner who determined the secrecy capacity for the non-degraded *broadcast channel* (BC) with a single confidential message intended for one of the users [2].

In more general wireless network scenarios, secret communication may involve multiple users and multiple antennas. Motivated by wireless communication, where transmitted signals are broadcast and can be received by all users within the communication range, a significant research effort has been invested in the study of the information-theoretic limits of secret communication in different wireless network environments including multi-user communication with confidential messages [3]–[11], secret wireless communication on fading channels [12]–[15], and the Gaussian multiple-input single-output (MISO) and multiple-input multiple-output (MIMO) wiretap channels [16]–[21].

These issues motivate us to study the multi-antenna Gaussian BC with confidential messages (MGBC-CM), in which independent confidential messages from a multi-antenna transmitter are to be communicated to two users. The corresponding broadcast communication model is shown in Fig. 1. Each user would like to obtain its own message reliably and confidentially.

To give insight into this problem, we first consider a single-antenna Gaussian BC. Note that this channel is degraded [22], which means that if a message can be successfully decoded by the inferior user, then the

superior user is also ensured of decoding it. Hence, the secrecy rate of the inferior user is zero and this problem is reduced to the scalar Gaussian wiretap channel problem [23] whose secrecy capacity is now the maximum rate achievable by the superior user. This analysis gives rise to the question: can the transmitter, in fact, communicate with both users confidentially at nonzero rate under some other conditions? Roughly speaking, the answer is in the affirmative. In particular, the transmitter can communicate when equipped with sufficiently separated multiple antennas.

We here have two goals motivated directly by questions arising in practice. The first is to determine the condition under which both users can obtain their own confidential messages in a reliable and safe manner. This is equivalent to evaluating the secrecy capacity region for the MGBC-CM. The second is to show *how* the transmitter should broadcast confidentially, which is equivalent to designing an achievable secret coding scheme. To this end, we first describe a secret *dirty-paper coding* (DPC) scheme and derive the corresponding achievable secrecy rate region based on Gaussian codebooks. The secret DPC is based on *double-binning* [24] which enables both joint encoding and preserving confidentiality. Next, a computable Sato-type outer bound on the secrecy capacity region is developed for the MGBC-CM. Furthermore, the Sato-type outer bound prove to be consistent with the boundary of the secret dirty-paper coding achievable rate region, and hence, the secrecy capacity region of the MGBC-CM is established. Finally, two numerical examples demonstrate that both users can achieve positive rates simultaneously under the information-theoretic secrecy requirement.

The remainder of this paper is organized as follows. The system model and definitions are introduced in Section II. The main results on the secrecy capacity region of the MGBC-CM is state in Section III. The achievability proof associated with the secret DPC scheme is established in Section IV. The converse proof is derived in Section V based on the Sato-type outer bound. Finally, Section VI shows numerical examples and Section VII points our our conclusions.

II. System Model and Definitions

A. Channel Model

We consider the communication of confidential messages to two users over a Gaussian BC via $t \geq 2$ transmit-antennas. Each user is equipped with a single receive-antenna. As shown in Fig. 1, the transmitter sends independent confidential messages W_1 and W_2 in n channel uses with nR_1 and nR_2 bits, respectively. The message W_1 is destined for user 1 and eavesdropped by user 2, whereas the message W_2 is destined

for user 2 and eavesdropped by user 1. This communication scenario is referred to as the *multi-antenna Gaussian BC with confidential messages*. The Gaussian BC is an additive noise channel and the received symbols at user 1 and user 2 are represented using the following expression:

$$\begin{aligned} y_{1,i} &= \mathbf{h}^H \mathbf{x}_i + z_{1,i} \\ y_{2,i} &= \mathbf{g}^H \mathbf{x}_i + z_{2,i}, \qquad i = 1, \dots, n \end{aligned} \tag{1}$$

where $\mathbf{x}_i \in \mathbb{C}^t$ is a complex input vector at time i, $\{z_{1,i}\}$ and $\{z_{2,i}\}$ correspond to two independent, zero-mean, unit-variance, complex Gaussian noise sequences, and $\mathbf{h}, \mathbf{g} \in \mathbb{C}^t$ are fixed, complex channel attenuation vectors imposed on user 1 and user 2, respectively. The channel input is constrained by $\mathrm{tr}(K_{\mathbf{X}}) \leq P$, where P is the average total power limitation at the transmitter. We also assume that both the transmitter and users are aware of the attenuation vectors.

B. Important Channel Parameters for the MGBC-CM

For the MGBC-CM, we are interested in the following important parameters, which are related to the generalized eigenvalue problem (see Appendix I for the details).

Let λ_1 and $\mathbf{e}_1$ denote the largest generalized eigenvalue and the corresponding normalized eigenvector of the pencil $(I + P\mathbf{h}\mathbf{h}^H, I + P\mathbf{g}\mathbf{g}^H)$ so that $\mathbf{e}_1^H \mathbf{e}_1 = 1$ and

$$(I + P\mathbf{h}\mathbf{h}^H)\mathbf{e}_1 = \lambda_1 (I + P\mathbf{g}\mathbf{g}^H)\mathbf{e}_1. \tag{2}$$

Similarly, we define λ_2 and $\mathbf{e}_2$ as the largest generalized eigenvalue and the corresponding normalized eigenvector of the pencil $(I + P\mathbf{g}\mathbf{g}^H, I + P\mathbf{h}\mathbf{h}^H)$ so that $\mathbf{e}_2^H \mathbf{e}_2 = 1$ and

$$(I + P\mathbf{g}\mathbf{g}^H)\mathbf{e}_2 = \lambda_2 (I + P\mathbf{h}\mathbf{h}^H)\mathbf{e}_2. \tag{3}$$

An useful property of λ_1 and λ_2 is described in the following lemma.

Lemma 1: For any channel attenuation vector pair $\mathbf{h}$ and $\mathbf{g}$, the largest generalized eigenvalues of the pencil $(I + P\mathbf{h}\mathbf{h}^H, I + P\mathbf{g}\mathbf{g}^H)$ and the pencil $(I + P\mathbf{g}\mathbf{g}^H, I + P\mathbf{h}\mathbf{h}^H)$ satisfy

$$\lambda_1 \geq 1 \quad \text{and} \quad \lambda_2 \geq 1. \tag{4}$$

Moreover, if $\mathbf{h}$ and $\mathbf{g}$ are linearly independent, then both λ_1 and λ_2 are strictly greater than 1.

Proof: We provide the proof in Appendix I. ■

C. *Definitions*

We now define the secret codebook, the probability of error, the secrecy level, and the secrecy capacity region for the MGBC-CM as follows.

An $(2^{nR_1}, 2^{nR_2}, n)$ *secret codebook* for the MGBC-CM consists of the following:

1) Two message sets $\mathcal{W}_1 = \{1, \ldots, 2^{nR_1}\}$ and $\mathcal{W}_2 = \{1, \ldots, 2^{nR_2}\}$.
2) An stochastic encoding function is specified by a matrix of conditional probability density $p(\mathbf{x}^n|w_1, w_2)$, where $\mathbf{x}^n = [\mathbf{x}_1, \ldots, \mathbf{x}_n] \in \mathbb{C}^{t\times n}$, $w_k \in \mathcal{W}_k$, and

$$\int_{\mathbf{x}^n} p(\mathbf{x}^n|w_1, w_2) = 1.$$

3) Decoding functions ϕ_1 and ϕ_2. The decoding function at user k is a deterministic mapping

$$\phi_k : \mathcal{Y}_k^n \to \mathcal{W}_k.$$

Remark 1: To increase the randomness of transmitted messages, we consider a *stochastic* encoder at the transmitter. In other words, $p(\mathbf{x}^n|w_1, w_2)$ is the conditional probability density that the messages (w_1, w_2) are jointly encoded as the channel input sequence $\mathbf{x}^n$.

At the receiver ends, the error performance and the secrecy level are evaluated by the following performance measures.

1) The reliability is measured by the maximum error probability

$$P_e^{(n)} \triangleq \max\big\{P_{e,1}^{(n)}, P_{e,2}^{(n)}\big\}$$

where $P_{e,k}^{(n)}$ is the error probability for user k given by

$$P_{e,k}^{(n)} = 2^{-n(R_1+R_2)} \sum_{w_1\in\mathcal{W}_1} \sum_{w_2\in\mathcal{W}_2} \Pr\big[\phi_k(Y_k^n) \neq w_k \big| (w_1, w_2) \text{ sent}\big]. \tag{5}$$

2) The secrecy levels with respect to confidential messages W_1 and W_2 are measured, respectively, at user 2 and user 1 with respect to the *equivocation rates*

$$\frac{1}{n}H(W_2|Y_1^n) \quad \text{and} \quad \frac{1}{n}H(W_1|Y_2^n). \tag{6}$$

A rate pair (R_1, R_2) is said to be achievable for the MGBC-CM if, for any $\epsilon > 0$, there exists an

$(2^{nR_1}, 2^{nR_2}, n)$ code that satisfies $P_e^{(n)} \leq \epsilon$, and the information-theoretic secrecy requirement[1]

$$\begin{aligned} & nR_1 - H(W_1|Y_2^n) \leq n\epsilon \\ \text{and} \quad & nR_2 - H(W_2|Y_1^n) \leq n\epsilon. \end{aligned} \tag{7}$$

The *secrecy capacity region* $\mathcal{C}_s^{\mathrm{MG}}$ of the MGBC-CM is the closure of the set of all achievable rate pairs (R_1, R_2).

III. Main Result: Secrecy Capacity Region for the MGBC-CM

The two-user Gaussian BC with multiple transmit-antennas is non-degraded. For this channel, we have the following closed-from result on the secrecy capacity region under the information-theoretic secrecy requirement.

Theorem 1: We consider an MGBC-CM modeled in (1). Let

$$\gamma_1(\alpha) = \frac{1 + \alpha P|\mathbf{h}^H \mathbf{e}_1|^2}{1 + \alpha P|\mathbf{g}^H \mathbf{e}_1|^2}, \tag{8}$$

$\gamma_2(\alpha)$ be the largest generalized eigenvalue of the pencil

$$\left(I + \frac{(1-\alpha)P}{1 + \alpha P|\mathbf{g}^H \mathbf{e}_1|^2} \mathbf{g}\mathbf{g}^H,\ I + \frac{(1-\alpha)P}{1 + \alpha P|\mathbf{h}^H \mathbf{e}_1|^2} \mathbf{h}\mathbf{h}^H \right), \tag{9}$$

and $\mathcal{R}^{\mathrm{MG}}(\alpha)$ denote the union of all (R_1, R_2) satisfying

$$\begin{aligned} & 0 \leq R_1 \leq \log_2 \gamma_1(\alpha) \\ \text{and} \quad & 0 \leq R_2 \leq \log_2 \gamma_2(\alpha). \end{aligned} \tag{10}$$

The secrecy capacity region of the MGBC-CM is

$$\mathcal{C}_s^{\mathrm{MG}} = \mathrm{co} \left\{ \bigcup_{0 \leq \alpha \leq 1} \mathcal{R}^{\mathrm{MG}}(\alpha) \right\}, \tag{11}$$

where $\mathrm{co}\{\mathcal{S}\}$ denotes the convex hull of the set $\mathcal{S}$.

Proof: We provide the achievability proof in Section IV based on a secret dirty paper coding scheme, and show the converse proof in Section V based on a Sato-type outer bound. ■

[1] This definition corresponds to the so-called *weak secrecy-key rate* [25]. A stronger measurement of the secrecy level has been defined by Maurer and Wolf in terms of absolute equivocation [25], where the authors have shown that the former definition could replaced by the latter without any rate penalty in a wiretap channel.

Based on Theorem 1, we can calculate the boundary of the secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ by choosing α to trade off the rate R_1 for the rate R_2. In particular, when $\alpha = 1$, we obtain

$$\gamma_1(1) = \frac{\mathbf{e}_1^H(I + P\mathbf{h}\mathbf{h}^H)\mathbf{e}_1}{\mathbf{e}_1^H(I + P\mathbf{g}\mathbf{g}^H)\mathbf{e}_1} = \lambda_1 \tag{12}$$

and

$$\gamma_2(1) = 1 \tag{13}$$

where (12) follows from the definitions of λ_1 and $\mathbf{e}_1$ in (2). Theorem 1 implies that the rate pair $(\log_2 \lambda_1, 0)$ is achievable. In fact, this rate pair is the corner point corresponding to the maximum achievable rate of user 1 in the capacity region $\mathcal{C}_s^{\mathrm{MG}}$.

Corollary 1: For the MGBC-CM, the maximum secrecy rate of user 1 is given by

$$R_{1,\max} = \max_{0 \le \alpha \le 1} \log_2 \gamma_1(\alpha) = \log_2 \lambda_1 \tag{14}$$

where λ_1 is the largest generalized eigenvalue of the pencil $(I + P\mathbf{h}\mathbf{h}^H, I + P\mathbf{g}\mathbf{g}^H)$.

Proof: See Appendix II. ■

Example 1: (MISO Wiretap Channels) A special case of the MGBC-CM model is the Gaussian MISO wiretap channel studied in [16], [18], [20], where the transmitter sends confidential information to only one user and treats another user as an eavesdropper. Let us consider a Gaussian MISO wiretap channel modeled in (1), where user 1 is the legitimate receiver and user 2 is the eavesdropper. Corollary 1 implies that the secrecy capacity of the Gaussian MISO wiretap channel corresponds to the corner point of $\mathcal{C}_s^{\mathrm{MG}}$. Hence, the secrecy capacity of the Gaussian MISO wiretap channel is given by

$$C_s^{\mathrm{MISO}} = \log_2 \lambda_1, \tag{15}$$

which coincides with the result of [18].

For the MGBC-CM, the actions of user 1 and user 2 are symmetric to each other, i.e., each user decodes its own message and eavesdrops the confidential information belonging to another user. Based on symmetry of this two-user BC model, we can express the secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ in an alternative way.

Corollary 2: For an MGBC-CM modeled in (1), the secrecy capacity region can be written as

$$\mathcal{C}_s^{\mathrm{MG}} = \mathrm{co}\left\{ \bigcup_{0 \le \beta \le 1} \mathcal{R}^{\mathrm{MG-2}}(\beta) \right\} \tag{16}$$

where $\mathcal{R}^{\mathrm{MG}-2}(\beta)$ denotes the union of all (R_1, R_2) satisfying

$$0 \le R_1 \le \log_2 \xi_1(\beta)$$
$$\text{and} \qquad 0 \le R_2 \le \log_2 \xi_2(\beta), \tag{17}$$

$\xi_1(\beta)$ is the largest generalized eigenvalue of the pencil

$$\left(I + \frac{(1-\beta)P}{1+\beta P|\mathbf{h}^H \mathbf{e}_2|^2} \mathbf{h}\mathbf{h}^H,\ I + \frac{(1-\beta)P}{1+\beta P|\mathbf{g}^H \mathbf{e}_2|^2} \mathbf{g}\mathbf{g}^H \right) \tag{18}$$

and

$$\xi_2(\beta) = \frac{1+\beta P|\mathbf{g}^H \mathbf{e}_2|^2}{1+\beta P|\mathbf{h}^H \mathbf{e}_2|^2}. \tag{19}$$

Proof: The derivation follows from the same approach of the proof for Theorem 1 by reversing the roles of user 1 and user 2. ■

Remark 2: Theorem 1 and Corollary 2 imply that if α and β satisfy the implicit function $\gamma_1(\alpha) = \xi_1(\beta)$, then

$$\mathcal{R}^{\mathrm{MG}}(\alpha) = \mathcal{R}^{\mathrm{MG}-2}(\beta).$$

For example, it is easy to check $\mathcal{R}^{\mathrm{MG}}(1) = \mathcal{R}^{\mathrm{MG}-2}(0)$.

Now, by applying Corollary 2 and setting $\beta = 1$, we can show that the rate pair $(0, \log_2 \lambda_2)$ is the corner point corresponding to the maximum achievable rate of user 2 in the capacity region $\mathcal{C}_s^{\mathrm{MG}}$.

Corollary 3: For the MGBC-CM, the maximum secrecy rate of user 2 is given by

$$R_{2,\max} = \log_2 \lambda_2 \tag{20}$$

where λ_2 is the largest generalized eigenvalue of the pencil $(I + P\mathbf{g}\mathbf{g}^H, I + P\mathbf{h}\mathbf{h}^H)$.

Proof: The derivation follows from the same approach of the proof for Corollary 1. ■

Corollaries 1 and 3 imply that for the MGBC-CM, both users can achieve positive rates with information-theoretic secrecy if and only if $\lambda_1 > 1$ and $\lambda_2 > 1$. Lemma 1 illusrtates that this condition can be ensured when the attenuation vectors $\mathbf{h}$ and $\mathbf{g}$ are linear independent.

IV. Secret DPC Coding Scheme and Achievability Proof

We first briefly review the prior information-theoretic result on the achievable rate region for the *BC with confidential messages* (BC-CM) of [24]. Based on this result, we develop the achievable secret coding

scheme for the MGBC-CM and find the capacity achieving input covariance matrix.

A. Double-Binning Inner bound for the BC-CM

An achievable rate region for the BC-CM has been established in [24] based on a double-binning scheme that enables both joint encoding at the transmitter by using Slepian-Wolf binning [26] and preserving confidentiality by using random binning. We summarize the double-binning codebook and encoding strategy in Appendix III for completeness.

Lemma 2: ([24, Theorem 3]) Let $\mathbf{V}_1$ and $\mathbf{V}_2$ be auxiliary random variables, Ω denote the class of joint probability densities $p(\mathbf{v}_1, \mathbf{v}_2, \mathbf{x}, y_1, y_2)$ that factor as

$$p(\mathbf{v}_1, \mathbf{v}_2)p(\mathbf{x}|\mathbf{v}_1, \mathbf{v}_2)p(y_1, y_2|\mathbf{x}), \tag{21}$$

and $\mathcal{R}_{\mathrm{I}}(\pi)$ denote the union of all (R_1, R_2) satisfying

$$0 \leq R_1 \leq I(\mathbf{V}_1; Y_1) - I(\mathbf{V}_1; Y_2|\mathbf{V}_2) - I(\mathbf{V}_1; \mathbf{V}_2) \tag{22}$$

$$\text{and} \qquad 0 \leq R_2 \leq I(\mathbf{V}_2; Y_2) - I(\mathbf{V}_2; Y_1|\mathbf{V}_1) - I(\mathbf{V}_1; \mathbf{V}_2) \tag{23}$$

for a given joint probability density $\pi \in \Omega$. For the BC-CM, any rate pair

$$(R_1, R_2) \in \mathrm{co}\left\{ \bigcup_{\pi \in \Omega} \mathcal{R}_{\mathrm{I}}(\pi) \right\} \tag{24}$$

is achievable.

The proof of Lemma 2 can be found in [24]. Here, we provide an alternative view on this result. Since randomization can increase secrecy, we employ stochastic encoding at the transmitter so that the size of the secret codebook is larger than the size of message set. Let R' denote the redundant rate used to prevent the confidentiality. The best known achievable region for a general BC was found by Marton of [27]. Now, for a given joint density $p(\mathbf{v}_1, \mathbf{v}_2, \mathbf{x})$, a special case of the Marton sum rate (without a common rate) is given by

$$R_1 + R_2 + R' \leq I(\mathbf{V}_1; Y_1) + I(\mathbf{V}_2; Y_2) - I(\mathbf{V}_1; \mathbf{V}_2). \tag{25}$$

On the other hand, the total (both the intended and the eavesdropped) information rate obtained by user 2 is limited by $I(\mathbf{V}_1, \mathbf{V}_2; Y_2)$. Intuitively, to keep the message W_1 secret from user 2, the redundant rate R'

should satisfy that

$$R_2 + R' \geq I(\mathbf{V}_1, \mathbf{V}_2; Y_2). \tag{26}$$

This implies that to satisfy the information-theoretic secrecy requirement, the achievable secrecy rate of user 1 can be written as

$$R_1 \leq [I(\mathbf{V}_1; Y_1) + I(\mathbf{V}_2; Y_2) - I(\mathbf{V}_1; \mathbf{V}_2)] - I(\mathbf{V}_1, \mathbf{V}_2; Y_2). \tag{27}$$

Similarly, the achievable secrecy rate of user 2 can be written as

$$R_2 \leq [I(\mathbf{V}_1; Y_1) + I(\mathbf{V}_2; Y_2) - I(\mathbf{V}_1; \mathbf{V}_2)] - I(\mathbf{V}_1, \mathbf{V}_2; Y_1). \tag{28}$$

Bounds (27) and (28) lead to the achievable secrecy rate region in Lemma 2.

Remark 3: For the BC with confidential messages, one can employ joint encoding at the transmitter. However, to preserve confidentiality, both achievable rate expressions in (22) and (23) include a penalty term $I(\mathbf{V}_1; \mathbf{V}_2)$. Hence, compared with Marton's achievable region [27] for a general BC, here, one need to pay "double" for jointly encoding at the transmitter.

B. Secret DPC Scheme for the MGBC-CM

The achievable strategy in Lemma 2 introduces a double-binning coding scheme. However, when the rate region (24) is used as a constructive technique, it not clear how to choose the auxiliary random variables $\mathbf{V}_1$ and $\mathbf{V}_2$ to implement the double-binning codebook, and hence, one has to "guess" the density of $p(\mathbf{v}_1, \mathbf{v}_2, \mathbf{x})$. Here, we employ the DPC technique with the double-binning code structure to develop the *secret DPC* (S-DPC) achievable rate region for the MGBC-CM.

For the MGBC-CM, we consider a secret dirty-paper encoder with Gaussian codebooks as follows. First, we sperate the channel input $\mathbf{X}$ into two random vectors $\mathbf{U}_1$ and $\mathbf{U}_2$ so that

$$\mathbf{U}_1 + \mathbf{U}_2 = \mathbf{X}. \tag{29}$$

We choose $\mathbf{U}_1$ and $\mathbf{U}_2$ as well as auxiliary random variables $\mathbf{V}_1$ and $\mathbf{V}_2$ as follows:

$$\begin{aligned}
&\mathbf{U}_1 \sim \mathcal{CN}(0, K_{\mathbf{U}_1}),\\
&\mathbf{U}_2 \sim \mathcal{CN}(0, K_{\mathbf{U}_2}),\ \text{ independent of } \mathbf{U}_1\\
&\mathbf{V}_1 = \mathbf{U}_1 + \mathbf{b}\mathbf{h}^H\mathbf{U}_2 \quad \text{and} \quad \mathbf{V}_2 = \mathbf{U}_2
\end{aligned} \tag{30}$$

where $K_{\mathbf{U}_1}$ and $K_{\mathbf{U}_2}$ are covariance matrices of $\mathbf{U}_1$ and $\mathbf{U}_2$, respectively, and

$$\mathbf{b} = \frac{K_{\mathbf{U}_1}\mathbf{h}}{1 + \mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}. \tag{31}$$

Based on the conditions (30) and Lemma 2, we obtain a S-DPC rate region for the MGBC-CM as follows.

Lemma 3: [S-DPC region] Let $\mathcal{R}_{\mathrm{I}}^{\mathrm{S-DPC}}(K_{\mathbf{U}_1}, K_{\mathbf{U}_2})$ denote the union of all (R_1, R_2) satisfying

$$0 \leq R_1 \leq \log_2 \frac{1 + \mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}{1 + \mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}} \tag{32}$$

and

$$0 \leq R_2 \leq \log_2 \frac{1 + \mathbf{g}^H (K_{\mathbf{U}_1} + K_{\mathbf{U}_2})\mathbf{g}}{1 + \mathbf{h}^H (K_{\mathbf{U}_1} + K_{\mathbf{U}_2})\mathbf{h}} + \log_2 \frac{1 + \mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}{1 + \mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}}. \tag{33}$$

Then, any rate pair

$$(R_1, R_2) \in \mathrm{co}\left\{ \bigcup_{\mathrm{tr}(K_{\mathbf{U}_1} + K_{\mathbf{U}_2}) \leq P} \mathcal{R}_{\mathrm{I}}^{\mathrm{S-DPC}}(K_{\mathbf{U}_1}, K_{\mathbf{U}_2}) \right\} \tag{34}$$

is achievable for the MGBC-CM.

Proof: See the Appendix III. ■

Remark 4: We choose the random variables $\mathbf{U}_1$, $\mathbf{U}_2$, $\mathbf{V}_1$, $\mathbf{V}_2$ and $\mathbf{X}$ as the same as the classical DPC strategy (e.g., see [28], [29]). However, the S-DPC scheme is different from the classical one. The codebook and the coding structure of the S-DPC scheme is based on the double-binning (see Appendix III).

C. Achievability Proof of Theorem 1

The S-DPC achievable rate region (34) requires optimization of the covariance matrices $K_{\mathbf{U}_1}$ and $K_{\mathbf{U}_2}$. In order to achievable the boundary of $\mathcal{C}_s^{\mathrm{MG}}$, we choose $K_{\mathbf{U}_1}$ and $K_{\mathbf{U}_2}$ as follows:

$$K_{\mathbf{U}_1} = \alpha P \mathbf{e}_1 \mathbf{e}_1^H$$

and

$$K_{\mathbf{U}_2} = (1-\alpha) P \mathbf{c}_2(\alpha)\mathbf{c}_2^H(\alpha), \qquad \text{for } 0 \leq \alpha \leq 1 \tag{35}$$

where $\mathbf{e}_1$ is defined in (2) and $\mathbf{c}_2(\alpha)$ is a normalized eigenvector of the pencil (9) corresponding to $\gamma_2(\alpha)$ so that $\mathbf{c}_2^H(\alpha)\mathbf{c}_2(\alpha) = 1$ and

$$\left(I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H\right)\mathbf{c}_2(\alpha) = \gamma_2(\alpha)\left(I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right)\mathbf{c}_2(\alpha). \tag{36}$$

Since $\mathbf{U}_1$ and $\mathbf{U}_2$ are independent, (29) implies that the input covariance matrix can be written as follows:

$$\begin{aligned} K_{\mathbf{X}} &= K_{\mathbf{U}_1} + K_{\mathbf{U}_2} \\ &= \alpha P\mathbf{e}_1\mathbf{e}_1^H + (1-\alpha)P\mathbf{c}_2(\alpha)\mathbf{c}_2^H(\alpha), \qquad \text{for } 0 \le \alpha \le 1. \end{aligned} \tag{37}$$

Hence, we have

$$\mathrm{tr}(K_{\mathbf{X}}) = \mathrm{tr}(K_{\mathbf{U}_1} + K_{\mathbf{U}_2}) = P, \tag{38}$$

i.e., the channel input power constraint is satisfied.

Next, inserting (35) into (32) and (33), we obtain

$$\frac{1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}{1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}} = \gamma_1(\alpha) \tag{39}$$

and

$$\frac{[1+\mathbf{g}^H(K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{g}][1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}]}{[1+\mathbf{h}^H(K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{h}][1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}]} = \gamma_2(\alpha). \tag{40}$$

where the intermediate steps for deriving (40) are given in Appendix III. Now, by substituting (39) and (40) into Lemma 3, we obtain the desired achievable result.

Remark 5: The secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ can be achieved by using the S-DPC scheme, in which the capacity achieving input covariance matrix is with rank 2. Furthermore, by reversing the roles of user 1 and user 2, we have the achievability proof for Corollary 2.

V. Sato-Type Outer Bound and Converse Proof

In this section, we first describe a new Sato-type outer bound that can be applied to both discrete memoryless and Gaussian broadcast channels with confidential messages. Next, a computable Gaussian version of this bound is derived for the MGBC-CM. Finally, we prove that the Sato-type outer bound coincides with the secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$.

A. Sato-Type Outer Bound

We consider an important property for the BC-CM in the following lemma.

Lemma 4: Let $\mathcal{P}$ denote the set of channels $p_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}}$ whose marginal distributions satisfy

$$p_{\tilde{Y}_1|\mathbf{X}}(y_1|\mathbf{x}) = p_{Y_1|\mathbf{X}}(y_1|\mathbf{x})$$
$$\text{and} \qquad p_{\tilde{Y}_2|\mathbf{X}}(y_2|\mathbf{x}) = p_{Y_1|\mathbf{X}}(y_2|\mathbf{x}) \tag{41}$$

for all y_1, y_2 and $\mathbf{x}$. The secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ is the same for the channels $p_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}} \in \mathcal{P}$.

Proof: We provide the proof in Appendix III. ∎

We note that $\mathcal{P}$ is the set of channels $p_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}}$ that have the same marginal distributions as the original channel transition density $p_{Y_1,Y_2|\mathbf{X}}$. Lemma 4 implies that the secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ depends only on marginal distributions.

Theorem 2: Let $\mathcal{R}_{\mathrm{O}}\left(P_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}}, P_{\mathbf{X}}\right)$ denote the union of all rate pairs (R_1, R_2) satisfying

$$R_1 \leq I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2) - I(\mathbf{X};\tilde{Y}_2) \tag{42}$$
$$\text{and} \qquad R_2 \leq I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2) - I(\mathbf{X};\tilde{Y}_1) \tag{43}$$

for given distributions $P_{\mathbf{X}}$ and $P_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}}$. The secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ of the BC-CM satisfies

$$\mathcal{C}_s^{\mathrm{MG}} \subseteq \bigcap_{P_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}} \in \mathcal{P}} \left\{ \bigcup_{P_{\mathbf{X}}} \mathcal{R}_{\mathrm{O}}\left(P_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}}, P_{\mathbf{X}}\right) \right\}. \tag{44}$$

Proof: See the Appendix III. ∎

Remark 6: The outer bound (44) follows by evaluating the secrecy level at each user end in an individual manner, while by letting the users decode their messages in a *cooperative* manner. In this sense, we refer to this bound as “Sato-type” outer bound.

For example, we consider the confidential message W_1 that is destined for user 1 (corresponding to $\tilde{Y}_1$) and eavesdropped by user 2 (corresponding to $\tilde{Y}_2$). We assume that a genie gives user 1 the signal $\tilde{Y}_2$ as the side information for decoding W_1. Note that the eavesdropped signal $\tilde{Y}_2$ at user 2 is always a degraded version of the entire received signal $(\tilde{Y}_1, \tilde{Y}_2)$. This permits the use of the wiretap channel result of [1].

Remark 7: Although Theorem 2 is based on a *degraded* argument, the outer bound (44) can be applied to *general* broadcast channels with confidential messages.

B. Sato-Type Outer Bound for the MGBC-CM

For the Gaussian BC, the family $\mathcal{P}$ is the set of channels

$$\begin{aligned}\tilde{y}_1 &= \mathbf{h}^H\mathbf{x} + \tilde{z}_1\\ \tilde{y}_2 &= \mathbf{g}^H\mathbf{x} + \tilde{z}_2\end{aligned} \tag{45}$$

where $\tilde{z}_1$ and $\tilde{z}_2$ correspond to arbitrarily correlated, zero-mean, unit-variance, complex Gaussian random variables. Let ρ denote the covariance between $\tilde{Z}_1$ and $\tilde{Z}_2$, i.e,

$$\mathrm{Cov}\big(\tilde{Z}_1, \tilde{Z}_2\big) = \rho \quad \text{and} \quad |\rho|^2 \le 1.$$

Now, the rate region $\mathcal{R}_{\mathrm{O}}\big(P_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}}, P_{\mathbf{X}}\big)$ is a function of the noise covariance ρ and the input covariance matrix $K_{\mathbf{X}}$. We consider a computable Sato-type outer bound for the MGBC-CM in the following lemma.

Lemma 5: Let $\mathcal{R}_{\mathrm{O}}^{\mathrm{MG}}(\rho, K_{\mathbf{X}})$ denote the union of all rate pairs (R_1, R_2) satisfying

$$0 \le R_1 \le f_1(\rho, K_{\mathbf{X}}) \tag{46}$$

$$\text{and} \qquad 0 \le R_2 \le f_2(\rho, K_{\mathbf{X}}) \tag{47}$$

where

$$f_1(\rho, K_{\mathbf{X}}) = \min_{\nu\in\mathbb{C}} \log_2 \frac{(\mathbf{h}-\nu\mathbf{g})^H K_{\mathbf{X}}(\mathbf{h}-\nu\mathbf{g}) + 1 + |\nu|^2 - \nu^*\rho - \rho^*\nu}{(1-|\rho|^2)} \tag{48}$$

$$\text{and} \qquad f_2(\rho, K_{\mathbf{X}}) = \min_{\mu\in\mathbb{C}} \log_2 \frac{(\mathbf{g}-\mu\mathbf{h})^H K_{\mathbf{X}}(\mathbf{g}-\mu\mathbf{h}) + 1 + |\mu|^2 - \mu^*\rho - \rho^*\mu}{(1-|\rho|^2)}. \tag{49}$$

For the MGBC-CM, the secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ satisfies

$$\mathcal{C}_s^{\mathrm{MG}} \subseteq \bigcup_{\mathrm{tr}(K_{\mathbf{X}})\le P} \mathcal{R}_{\mathrm{O}}(\rho, K_{\mathbf{X}}) \tag{50}$$

for any $0 \le |\rho| \le 1$.

Proof: We provide the proof in Appendix III. ■

C. Converse Proof of Theorem 1

In this subsection, we prove that the Sato-type outer bound of Lemma 5 coincides with the secrecy capacity region $\mathcal{C}_s^{\mathrm{MG}}$ by properly choosing the parameter ρ.

1) Choosing the parameter ρ: Note that Lemma 5 is true for any ρ such that $0 \leq |\rho| \leq 1$. In particular, we consider

$$\rho_{\rm o} \triangleq \frac{\mathbf{g}^H \mathbf{e}_1}{\mathbf{h}^H \mathbf{e}_1}. \tag{51}$$

The definitions of λ_1 and $\mathbf{e}_1$ in (2) imply that

$$|\mathbf{h}^H \mathbf{e}_1|^2 - \lambda_1 |\mathbf{g}^H \mathbf{e}_1|^2 = \frac{\lambda_1 - 1}{P}. \tag{52}$$

Since $\lambda_1 \geq 1$ (see Lemma 1), we obtain

$$\left| \frac{\mathbf{g}^H \mathbf{e}_1}{\mathbf{h}^H \mathbf{e}_1} \right| \leq 1. \tag{53}$$

Hence, we can choose $\rho = \rho_{\rm o}$ in Lemma 5.

2) Determining the relationship between $K_{\mathbf{X}}$ and α: We observe that the rate region $\mathcal{R}_{\rm O}^{\rm MG}(\rho_{\rm o}, K_{\mathbf{X}})$ defined in Lemma 5 is a function of the input covariance matrix $K_{\mathbf{X}}$, while the rate region $\mathcal{R}^{\rm MG}(\alpha)$ defined in Theorem 1 is a function of α. In order to prove the main result, we build the relationship between $K_{\mathbf{X}}$ and α in the following lemma.

Lemma 6: For any input covariance matrix $K_{\mathbf{X}}$ with $\mathrm{tr}(K_{\mathbf{X}}) \leq P$, there exists a $\alpha \in [0, 1]$ such that $L(K_{\mathbf{X}}, \alpha) = 0$, where

$$L(K_{\mathbf{X}}, \alpha) = [\mathbf{h} - \rho_{\rm o} \gamma_1(\alpha) \mathbf{g}]^H (K_{\mathbf{X}} - \alpha P \mathbf{e}_1 \mathbf{e}_1^H) [\mathbf{h} - \rho_{\rm o} \gamma_1(\alpha) \mathbf{g}]. \tag{54}$$

Proof: We provide the proof in Appendix IV. ■

Based on the function $L(\cdot)$, we define the subset of input covariance matrices in terms of α as follows:

$$\mathcal{L}(\alpha) = \{K_{\mathbf{X}} : \; L(K_{\mathbf{X}}, \alpha) = 0\}. \tag{55}$$

Moreover, Lemma 6 implies that

$$\bigcup_{0 \leq \alpha \leq 1} \mathcal{L}(\alpha) = \{K_{\mathbf{X}} : \; \mathrm{tr}(K_{\mathbf{X}}) \leq P\}. \tag{56}$$

3) Bound on $f_1(\rho_{\rm o}, K_{\mathbf{X}})$: Now, we prove that if $K_{\mathbf{X}} \in \mathcal{L}(\alpha)$, then

$$f_1(\rho_{\rm o}, K_{\mathbf{X}}) \leq \log_2 \gamma_1(\alpha). \tag{57}$$

Let $\nu(\alpha)=\rho_{\rm o}\gamma_1(\alpha)$. For a given $K_{\mathbf{X}}\in\mathcal{L}(\alpha)$, the definition (48) implies that

$$\begin{aligned} f_1(\rho_{\rm o},K_{\mathbf{X}}) &\le \log_2\frac{[\mathbf{h}-\nu(\alpha)\mathbf{g}]^H K_{\mathbf{X}}[\mathbf{h}-\nu(\alpha)\mathbf{g}]+1+|\nu(\alpha)|^2-\nu^*(\alpha)\rho_{\rm o}-\rho_{\rm o}^*\nu(\alpha)}{1-|\rho_{\rm o}|^2}\\ &=\log_2\frac{\alpha P\left|[\mathbf{h}-\rho_{\rm o}\gamma_1(\alpha)\mathbf{g}]^H\mathbf{e}_1\right|^2+1+|\rho_{\rm o}|^2\gamma_1^2(\alpha)-2|\rho_{\rm o}|^2\gamma_1(\alpha)}{1-|\rho_{\rm o}|^2}. \end{aligned} \tag{58}$$

Based on the definition of $\rho_{\rm o}$ in (51), we have

$$\begin{aligned} \mathbf{h}-\rho_{\rm o}\gamma_1(\alpha)\mathbf{g} &= \mathbf{h}-\gamma_1(\alpha)\frac{\mathbf{g}\mathbf{g}^H\mathbf{e}_1}{\mathbf{h}^H\mathbf{e}_1}\\ &=\left[\frac{\mathbf{h}\mathbf{h}^H-\gamma_1(\alpha)\mathbf{g}\mathbf{g}^H}{\mathbf{h}^H\mathbf{e}_1}\right]\mathbf{e}_1. \end{aligned} \tag{59}$$

Hence,

$$\begin{aligned} \left|[\mathbf{h}-\rho_{\rm o}\gamma_1(\alpha)\mathbf{g}]^H\mathbf{e}_1\right|^2 &= \frac{\left[|\mathbf{h}^H\mathbf{e}_1|^2-\gamma_1(\alpha)|\mathbf{g}^H\mathbf{e}_1|^2\right]^2}{|\mathbf{h}^H\mathbf{e}_1|^2}\\ &=\left[|\mathbf{h}^H\mathbf{e}_1|^2-\gamma_1(\alpha)|\mathbf{g}^H\mathbf{e}_1|^2\right]\left[1-\gamma_1(\alpha)|\rho_{\rm o}|^2\right]\\ &=\left[\frac{\gamma_1(\alpha)-1}{\alpha P}\right]\left[1-\gamma_1(\alpha)|\rho_{\rm o}|^2\right] \end{aligned} \tag{60}$$

where the last step of (60) follows from the definition of $\gamma_1(\alpha)$ in (8). Substituting (60) into (58), we obtain

$$\begin{aligned} f_1(\rho_{\rm o},K_{\mathbf{X}}) &\le \log_2\frac{[\gamma_1(\alpha)-1][1-\gamma_1(\alpha)|\rho_{\rm o}|^2]+1+|\rho_{\rm o}|^2\gamma_1^2(\alpha)-2|\rho_{\rm o}|^2\gamma_1(\alpha)}{1-|\rho_{\rm o}|^2}\\ &=\log_2\frac{\gamma_1(\alpha)-|\rho_{\rm o}|^2\gamma_1(\alpha)}{1-|\rho_{\rm o}|^2}\\ &=\log_2\gamma_1(\alpha). \end{aligned} \tag{61}$$

4) Bound on $f_2(\rho_{\rm o},K_{\mathbf{X}})$: Here, we prove that if $K_{\mathbf{X}}\in\mathcal{L}(\alpha)$, then

$$f_1(\rho_{\rm o},K_{\mathbf{X}})\le\log_2\gamma_2(\alpha) \tag{62}$$

where $\gamma_2(\alpha)$ is the largest generalized eigenvalue of the pencil (9). In fact, the smallest generalized eigenvalue of the pencil (9) is $\gamma_1(\alpha)/\lambda_1$. This result is described in the following lemma.

Lemma 7: $\gamma_1(\alpha)/\lambda_1$ and $\mathbf{e}_1(\alpha)$ are the smallest generalized eigenvalue and the corresponding normal-

ized eigenvector of the pencil

$$\left(I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H,\ I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right) \tag{63}$$

where λ_1 and $\mathbf{e}_1(\alpha)$ are defined in (2), and $\gamma_1(\alpha)$ is defined in (8).

Proof: We provide the proof in Appendix IV. ■

Based on the property of generalized eigenvalues (see Appendix I), Lemma 7 implies that

$$\mathbf{e}_1^H\left[I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H\right]\mathbf{c}_2(\alpha) = 0 \tag{64}$$

and

$$\mathbf{e}_1^H\left[I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right]\mathbf{c}_2(\alpha) = 0 \tag{65}$$

where $\mathbf{c}_2(\alpha)$ is the normalized eigenvector of the pencil (9) corresponding to $\gamma_2(\alpha)$. Hence,

$$\frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{e}_1^H\mathbf{g}\mathbf{g}^H\mathbf{c}_2(\alpha) = -\mathbf{e}_1^H\mathbf{c}_2(\alpha) \tag{66}$$

and

$$\frac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{e}_1^H\mathbf{h}\mathbf{h}^H\mathbf{c}_2(\alpha) = -\mathbf{e}_1^H\mathbf{c}_2(\alpha). \tag{67}$$

By combining the definitions of ρ_{o} in (51) and $\gamma_1(\alpha)$ in (8), we obtain

$$\rho_{\text{o}} = \frac{\mathbf{g}^H\mathbf{e}_1}{\mathbf{h}^H\mathbf{e}_1} = \frac{1}{\gamma_1(\alpha)}\left[\frac{\mathbf{h}^H\mathbf{c}_2(\alpha)}{\mathbf{g}^H\mathbf{c}_2(\alpha)}\right]^*. \tag{68}$$

We now establish the relationship between $\gamma_1(\alpha)$ and $\gamma_2(\alpha)$ based on (68) in the following lemma.

Lemma 8: For any $\alpha \in [0,1]$,

$$\frac{\mathbf{g} - \rho_{\text{o}}^*\gamma_2(\alpha)\mathbf{h}}{|\mathbf{g} - \rho_{\text{o}}^*\gamma_2(\alpha)\mathbf{h}|^2} = \mathbf{c}_2(\alpha) \tag{69}$$

and

$$[\mathbf{h} - \rho_{\text{o}}\gamma_1(\alpha)\mathbf{g}]^H[\mathbf{g} - \rho_{\text{o}}^*\gamma_2(\alpha)\mathbf{h}] = 0 \tag{70}$$

where $\gamma_1(\alpha)$ is defined in (8), and $\gamma_2(\alpha)$ and $\mathbf{c}_2(\alpha)$ are the largest generalized eigenvalue and the corresponding normalized eigenvector of the pencil (9).

Proof: We provide the proof in Appendix IV. ■

Let $\mathbf{c}_1(\alpha)$ denote the normalized vector of $\mathbf{h} - \rho_{\text{o}}\gamma_1(\alpha)\mathbf{g}$, i.e.,

$$\mathbf{c}_1(\alpha) \triangleq \frac{\mathbf{h} - \rho_{\text{o}}\gamma_1(\alpha)\mathbf{g}}{|\mathbf{h} - \rho_{\text{o}}\gamma_1(\alpha)\mathbf{g}|^2}. \tag{71}$$

Note that Lemma 8 implies that $\mathbf{c}_1(\alpha)$ and $\mathbf{c}_2(\alpha)$ are orthogonal. Moreover, since the input covariance matrix $K_{\mathbf{X}}$ is Hermitian and positive semidefinite, we obtain

$$\mathbf{c}_1^H(\alpha)K_{\mathbf{X}}\mathbf{c}_1(\alpha) + \mathbf{c}_2^H(\alpha)K_{\mathbf{X}}\mathbf{c}_2(\alpha) \leq \mathrm{tr}(K_{\mathbf{X}}) = P. \tag{72}$$

Hence, for a given $K_{\mathbf{X}} \in \mathcal{L}(\alpha)$, we have

$$\begin{aligned}\mathbf{c}_2^H(\alpha)K_{\mathbf{X}}\mathbf{c}_2(\alpha) &\leq P - \alpha P|\mathbf{c}_1^H(\alpha)\mathbf{e}_1|^2 \\ &= (1-\alpha)P + \alpha P|\mathbf{c}_2^H(\alpha)\mathbf{e}_1|^2.\end{aligned} \tag{73}$$

Inserting (69) into (73), we obtain

$$[\mathbf{g} - \rho_{\mathrm{o}}^*\gamma_2(\alpha)\mathbf{h}]^H K_{\mathbf{X}}[\mathbf{g} - \rho_{\mathrm{o}}^*\gamma_2(\alpha)\mathbf{h}] \leq (1-\alpha)P\zeta(\alpha) + \alpha P\eta(\alpha) \tag{74}$$

where

$$\zeta(\alpha) \triangleq |\mathbf{g} - \rho_{\mathrm{o}}^*\gamma_2(\alpha)\mathbf{h})|^2 \tag{75}$$

and

$$\eta(\alpha) \triangleq |\mathbf{g} - \rho_{\mathrm{o}}^*\gamma_2(\alpha)\mathbf{h}|^2|\mathbf{e}_1^H\mathbf{c}_2(\alpha)|^2. \tag{76}$$

In Appendix IV, we prove the following equality

$$(1-\alpha)P\zeta(\alpha) + \alpha P\eta(\alpha) = [\gamma_2(\alpha) - 1][1 - \gamma_2(\alpha)|\rho_{\mathrm{o}}|^2]. \tag{77}$$

Next, we consider the bound on $f_2(\rho_{\mathrm{o}}, K_{\mathbf{X}})$. Let

$$\mu(\alpha) = \rho_{\mathrm{o}}^*\gamma_2(\alpha).$$

For a given $K_{\mathbf{X}} \in \mathcal{L}(\alpha)$, the definition (49) implies that

$$\begin{aligned}f_2(\rho_{\mathrm{o}}, K_{\mathbf{X}}) &\leq \log_2 \frac{[\mathbf{g} - \mu(\alpha)\mathbf{h}]^H K_{\mathbf{X}}[\mathbf{g} - \mu(\alpha)\mathbf{h}] + 1 + |\mu(\alpha)|^2 - \mu^*(\alpha)\rho_{\mathrm{o}} - \rho_{\mathrm{o}}^*\mu(\alpha)}{1 - |\rho_{\mathrm{o}}|^2} \\ &\leq \log_2 \frac{(1-\alpha)P\zeta(\alpha) + \alpha P\eta(\alpha) + 1 + |\rho_{\mathrm{o}}|^2\gamma_2^2(\alpha) - 2|\rho_{\mathrm{o}}|^2\gamma_2(\alpha)}{1 - |\rho_{\mathrm{o}}|^2}.\end{aligned} \tag{78}$$

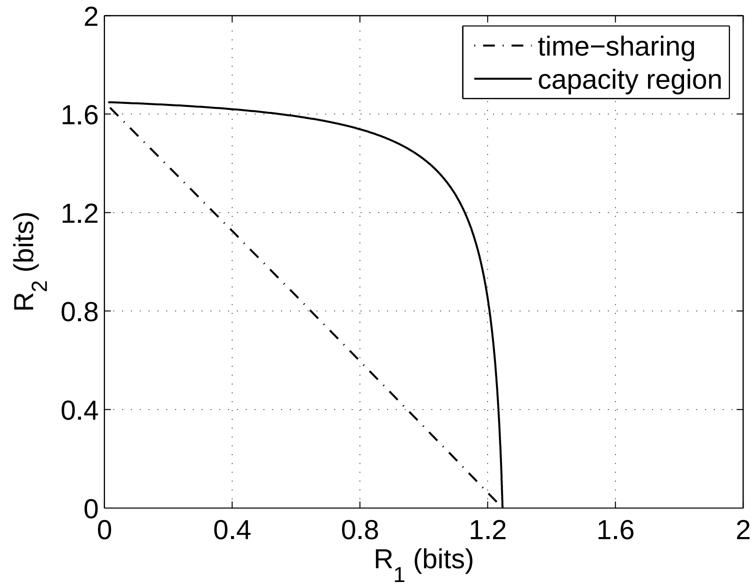

Fig. 2. Comparison of the Sato-type outer bound and secrecy rate regions achieved by time-sharing and simplified DPC schemes for the example MGBC-CM in (81)

Now, substituting (77) into (78), we obtain

$$\begin{aligned} f_2(\rho_{\rm o}, K_{\mathbf{X}}) &\leq \log_2 \frac{[\gamma_2(\alpha)-1][1-\gamma_2(\alpha)|\rho_{\rm o}|^2]+1+|\rho_{\rm o}|^2\gamma_2^2(\alpha)-2|\rho_{\rm o}|^2\gamma_2(\alpha)}{1-|\rho_{\rm o}|^2} \\ &= \log_2 \gamma_2(\alpha). \end{aligned} \tag{79}$$

Finally, Combining (56), (61) and (79), we have the desired result:

$$\bigcup_{\mathrm{tr}(K_{\mathbf{X}})\leq P} \mathcal{R}_{\rm O}(\rho, K_{\mathbf{X}}) \subseteq \bigcup_{0\leq\alpha\leq 1} \mathcal{R}^{\rm MG}(\alpha). \tag{80}$$

VI. Numerical Examples

In this section, we study two numerical examples to illustrate the secrecy capacity region of the MGBC-CM. For simplicity, we assume that the Gaussian BC has real input and output alphabets and the channel attenuation vectors $\mathbf{h}$ and $\mathbf{g}$ are real too. Under this condition, all calculated rate values are divided by 2.

Example 2: In the first example, we consider the following MGBC-CM

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1.5 & 0 \\ 1.801 & 0.871 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \tag{81}$$

where $\mathbf{h} = [1.5, 0]^T$, $\mathbf{g} = [1.801, 0.872]^T$, and the total power constraint is set to $P = 10$. Fig. 2 illustrates the secrecy capacity region for the channel (81). We observe that even though each component of the

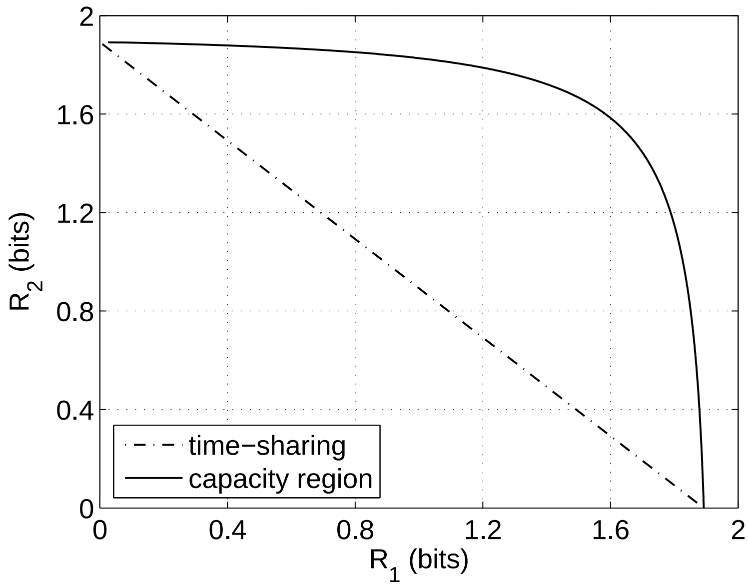

Fig. 3. Comparison of the Sato-type outer bound and secrecy rate regions achieved by time-sharing and simplified DPC schemes for the example MGBC-CM in (82)

attenuation vector $\mathbf{h}$ (imposed on user 1) is strictly less than the corresponding component of $\mathbf{g}$ (imposed on user 2), both users can achieve positive rates simultaneously under the information-theoretic secrecy requirement.

Example 3: In the second example, we consider the MGBC-CM as follows

$$\begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} 1.414 & 1.414 \\ 0.4 & 1.959 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} + \begin{bmatrix} z_1 \\ z_2 \end{bmatrix} \tag{82}$$

where $\mathbf{h} = [1.414, 1.414]^T$, $\mathbf{g} = [0.4, 1.959]^T$, and the total power $P = 10$. The secrecy capacity region of the channel (82) is calculated and depicted in Fig. 3.

Moreover, we compare the secrecy capacity region with the secrecy rate region achieved by the time-sharing scheme (indicated by the dash-dot line). The time-sharing refers to the scheme in which the transmitter sends the confidential message W_1 with total power P_1 during a fraction τ_1 of time, and sends the confidential message W_2 with total power P_2 during a fraction τ_2 of time, where

$$\tau_1 + \tau_2 = 1 \quad \text{and} \quad \tau_1 P_1 + \tau_2 P_2 = P.$$

Note that in each time fraction, the MGBC-CM reduces to a Gaussian MISO wiretap channel. Using such time-sharing, the rate pair $\left(\frac{\tau_1}{2}\log_2 \lambda_1(P_1), \frac{\tau_2}{2}\log_2 \lambda_2(P_2)\right)$ is achievable, where $\lambda_1(P_1)$ and $\lambda_2(P_2)$ are the largest generalized eigenvalues of the pencil $(I + P_1\mathbf{h}\mathbf{h}^H, I + P_1\mathbf{g}\mathbf{g}^H)$ and the pencil $(I +$

$P_2\mathbf{g}\mathbf{g}^H, I + P_2\mathbf{g}\mathbf{g}^H)$, respectively. Both Fig. 2 and Fig. 3 demonstrate that the time-sharing scheme is strictly suboptimal for providing the secrecy capacity region.

VII. CONCLUSION

In this paper, we have investigated the secrecy capacity region of a generally non-degraded Gaussian BC with confidential messages for two users, where the transmitter has t antennas and each user has a single antenna. For this model, we have proposed a secret dirty-paper coding scheme and introduced a computable Sato-type outer bound. Furthermore, we have proved that the boundary of the secret dirty-paper coding rate region is consistent with the Sato-type outer bound for the multiple-antenna Gaussian BC, and hence, we have obtained the secrecy capacity region for the MGBC-CM.

Unlike the single-antenna Gaussian BC-CM case, in which only the superior user can obtain confidential information at a positive secrecy rate, our result has illustrated that both users can achieve strictly positive rates with information-theoretic secrecy through a multiple-antenna Gaussian BC if attenuation vectors imposed on user 1 and user 2 are linear independent. Therefore, it becomes more practical and more attractive to achieve information-theoretic secrecy in wireless networks by employing multiple transmit-antennas at the physical layer.

APPENDIX I
THE GENERALIZED EIGENVALUE AND RAYLEIGH QUOTIENT PROBLEM

A generalized eigenvalue problem is to determine the nontrivial solutions of the equation

$$A\mathbf{e} = \lambda B\mathbf{e} \tag{83}$$

where A and B are matrices and λ is a scalar. The values of λ that satisfy (83) are the generalized eigenvalues and the corresponding vectors of $\mathbf{e}$ are the generalized eigenvectors.

In particular, if A is Hermitian and B is Hermitian and positive definite, then we have the following properties of $A\mathbf{e} = \lambda B\mathbf{e}$:

1) The generalized eigenvalues λ_i are real.
2) The eigenvectors are "B-orthogonal", i.e.,

$$\mathbf{e}_i^H B\mathbf{e}_j = 0 \quad \text{for } i \neq j. \tag{84}$$

3) Similarly,

$$\mathbf{e}_i^H A \mathbf{e}_j = \lambda_j \mathbf{e}_i^H A \mathbf{e}_j = 0 \quad \text{for } i \neq j. \tag{85}$$

Next, we describe the well-known *Rayleigh's quotient* [30] as follows.

Theorem 3: (see [30]) Let $r(\mathbf{c})$ be the Rayleigh's quotient defined as

$$r(\mathbf{c}) \triangleq \frac{\mathbf{c}^H A \mathbf{c}}{\mathbf{c}^H B \mathbf{c}}. \tag{86}$$

where A is Hermitian and B is Hermitian and positive definite. The quotient $R(\mathbf{c})$ is maximized by the eigenvector $\mathbf{e}_{\max}$ corresponding to the largest generalized eigenvalue $\lambda_{\max}$ of the pencil (A, B):

$$\max_{\mathbf{c}} R(\mathbf{c}) = \frac{\mathbf{e}_{\max}^H A \mathbf{e}_{\max}}{\mathbf{e}_{\max}^H B \mathbf{e}_{\max}} = \lambda_{\max} \tag{87}$$

and $R(\mathbf{c})$ is minimized by the eigenvector $\mathbf{e}_{\min}$ corresponding to the smallest generalized eigenvalue $\lambda_{\min}$ of the pencil (A, B):

$$\min_{\mathbf{c}} R(\mathbf{c}) = \frac{\mathbf{e}_{\min}^H A \mathbf{e}_{\min}}{\mathbf{e}_{\min}^H B \mathbf{e}_{\min}} = \lambda_{\min}. \tag{88}$$

The proof of Theorem 3 can be found in [30, Chapter 6]. Now we prove Lemma 1 based on the Rayleigh's quotient principle.

Proof: (**Lemma 1**) Since both $(I + P\mathbf{h}\mathbf{h}^H)$ and $(I + P\mathbf{g}\mathbf{g}^H)$ are Hermitian and positive definite matrices, the definition of λ_1 and Theorem 3 imply that

$$\lambda_1 = \max_{\mathbf{c}} \frac{\mathbf{c}^H (I + P\mathbf{h}\mathbf{h}^H) \mathbf{c}}{\mathbf{c}^H (I + P\mathbf{g}\mathbf{g}^H) \mathbf{c}}. \tag{89}$$

We consider a unit vector $\mathbf{c}_0$ that is orthogonal with the vector $\mathbf{g}$, i.e.,

$$\mathbf{c}_0^H \mathbf{c}_0 = 1 \quad \text{and} \quad \mathbf{c}_0^H \mathbf{g} = 0.$$

Now, we have

$$\begin{aligned} \lambda_1 &\geq \frac{\mathbf{c}_0^H (I + P\mathbf{h}\mathbf{h}^H) \mathbf{c}_0}{\mathbf{c}_0^H (I + P\mathbf{g}\mathbf{g}^H) \mathbf{c}_0} \\ &= 1 + P|\mathbf{c}_0^H \mathbf{h}|^2. \end{aligned} \tag{90}$$

This implies that $\lambda_1 \geq 1$. Furthermore, when $\mathbf{h}$ and $\mathbf{g}$ are linear independent, there exists a unit vector

$\mathbf{c}_0$ so that

$$\mathbf{c}_0^H \mathbf{g} = 0 \quad \text{and} \quad \mathbf{c}_0^H \mathbf{h} > 0. \tag{91}$$

Substituting (refeq:lg2) into (90), we obtain $\lambda_1 > 1$. By using the same approach, we can show that $\lambda_2 \geq 1$, and, in particular, $\lambda_2 > 1$ when $\mathbf{h}$ and $\mathbf{g}$ are linear independent. ■

APPENDIX II
PROOF OF COROLLARY 1

Proof: Theorem 1 demonstrates that for a given $\alpha \in [0, 1]$, the maximum achievable secrecy rate of user 1 is $\gamma_1(\alpha)$. This implies that

$$R_{1,\max} = \max_{0 \leq \alpha \leq 1} \gamma_1(\alpha). \tag{92}$$

We also notice that $\lambda_1 = \gamma_1(1)$. Hence, it is sufficient to show that $\gamma_1(\alpha)$ is a nondecreasing function on an interval $[0, 1]$.

Let

$$\kappa(\alpha) \triangleq \frac{d\gamma_1(\alpha)}{d\alpha}. \tag{93}$$

Based on the definition of $\gamma_1(\alpha)$ in (8), we can write

$$\begin{aligned} \kappa(\alpha) &= \frac{P|\mathbf{h}^H \mathbf{e}_1|^2(1 + \alpha P|\mathbf{g}^H \mathbf{e}_1|^2) - (1 + \alpha P|\mathbf{h}^H \mathbf{e}_1|^2)P|\mathbf{g}^H \mathbf{e}_1|^2}{(1 + \alpha P|\mathbf{g}^H \mathbf{e}_1|^2)^2} \\ &= \frac{P(|\mathbf{h}^H \mathbf{e}_1|^2 - |\mathbf{g}^H \mathbf{e}_1|^2)}{(1 + \alpha P|\mathbf{g}^H \mathbf{e}_1|^2)^2} \end{aligned} \tag{94}$$

Now, the definitions of λ_1 and $\mathbf{e}_1$ in (2) imply that

$$|\mathbf{h}^H \mathbf{e}_1|^2 - \lambda_1 |\mathbf{g}^H \mathbf{e}_1|^2 = \frac{\lambda_1 - 1}{P}. \tag{95}$$

Moreover, Since $\lambda_1 \geq 1$ (see Lemma 1), we obtain

$$\kappa(\alpha) \geq 0, \tag{96}$$

and hence, $\gamma_1(\alpha)$ is a nondecreasing function on an interval $[0,1]$. Therefore, we have

$$R_{1,\max} = \max_{0\leq\alpha\leq 1} \gamma_1(\alpha) = \lambda_1.$$

■

APPENDIX III
SECTION IV DERIVATIONS

(**Double-Binning Scheme**): By contrast with the classical DPC scheme, the secret DPC scheme is based on the double-binning code structure as follows. Let

$$R_1^\star = I(\mathbf{V}_1; Y_2|\mathbf{V}_2), \quad R_2^\star = I(\mathbf{V}_2; Y_1|\mathbf{V}_1) \quad \text{and} \quad R^\ddagger = I(\mathbf{V}_1; \mathbf{V}_2). \tag{97}$$

Generate $2^{n(R_k+R_k^\star+R^\ddagger)}$ codewords $\mathbf{v}_k^n(w_k, j_k, l_k)$, $w_k = 1, 2, \ldots, 2^{R_k}$, $j_k = 1, 2, \ldots, 2^{R_k^\star}$, $l_k = 1, 2, \ldots, 2^{R^\ddagger}$, independently at random according to $p(\mathbf{v}_k)$. Based on the labeling, we partition the codebook $\{\mathbf{v}_k^n(w_k, j_k, l_k)\}$ into 2^{nR_k} *bins*, where bin w_k represents the message index w_k. We further divide bin w_k into $2^{nR_k^\star}$ *sub-bins*. Each sub-bin (w_k, j_k) contains $2^{nR^\ddagger}$ codewords.

To send the message pair (w_1, w_2), the transmitter employs a joint stochastic encoder. We first randomly select a sub-bin (w_1, j_1) from the bin w_1 and randomly choose a codeword $\mathbf{v}_1^n(w_1, j_1, l_1)$ from the sub-bin (w_1, j_1). Next, we randomly select a sub-bin (w_2, j_2) from the bin w_2 and find a codeword $\mathbf{v}_2^n(w_2, j_2, l_2)$ in the sub-bin (w_2, j_2) so that the sequences $\mathbf{v}_1^n(w_1, j_1, l_1)$ and $\mathbf{v}_2^n(w_2, j_2, l_2)$ are jointly typical with respective to $p(\mathbf{v}_1, \mathbf{v}_2)$. Since each sub-bin contains $2^{nI(\mathbf{V}_1;\mathbf{V}_2)}$ codewords, the encoding is successful with probability close to 1 as long as n is large. Finally, we generate the channel input sequence $\mathbf{x}^n(w_1, w_2)$ according to the mapping $p(\mathbf{x}|\mathbf{v}_1, \mathbf{v}_2)$.

Proof: (**Lemma 3**) We first check the power constraint. Since $\mathbf{U}_1$ and $\mathbf{U}_2$ are independent and

$$\mathbf{X} = \mathbf{U}_1 + \mathbf{U}_2,$$

the covariance matrices $K_{\mathbf{U}_1}$ and $K_{\mathbf{U}_2}$ satisfy

$$\mathrm{tr}(K_{\mathbf{U}_1} + K_{\mathbf{U}_2}) = \mathrm{tr}(K_{\mathbf{X}}) \leq P. \tag{98}$$

Following from [29, Theorem 1] and using the setting in (30), we can immediately obtain the well-

known *successive dirty-paper encoding* result:

$$\begin{aligned} I(\mathbf{V}_1;Y_1) - I(\mathbf{V}_1;\mathbf{V}_2) &= I(\mathbf{U}_1;\mathbf{h}^H\mathbf{U}_1 + Z_1) \\ &= \log_2(1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}). \end{aligned} \tag{99}$$

Since $\mathbf{V}_2 = \mathbf{U}_2$ is independent of $\mathbf{U}_1$ and $\mathbf{V}_1 = \mathbf{U}_1 + \mathbf{b}\mathbf{h}^H\mathbf{U}_2$, we obtain

$$\begin{aligned} I(\mathbf{V}_1;Y_2|\mathbf{V}_2) &= I(\mathbf{U}_1 + \mathbf{b}\mathbf{h}^H\mathbf{U}_2;Y_2|\mathbf{U}_2) \\ &= I(\mathbf{U}_1;Y_2|\mathbf{U}_2) \\ &= \log_2(1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}). \end{aligned} \tag{100}$$

Combining (22), (99) and (100), we have

$$\begin{aligned} R_1 &\le I(\mathbf{V}_1;Y_1) - I(\mathbf{V}_1;\mathbf{V}_2) - I(\mathbf{V}_1;Y_2|\mathbf{V}_2) \\ &= \log_2 \frac{1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}{1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}}. \end{aligned} \tag{101}$$

Moreover, we can compute

$$\begin{aligned} I(\mathbf{V}_2;Y_2) &= h(Y_2) - h(Y_2|\mathbf{V}_2) \\ &= h(\mathbf{g}^H(\mathbf{U}_1+\mathbf{U}_2) + Z_2) - h(\mathbf{g}^H\mathbf{U}_1 + Z_2) \\ &= \log_2 \frac{1+\mathbf{g}^H (K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{g}}{1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}}. \end{aligned} \tag{102}$$

and

$$\begin{aligned} I(\mathbf{V}_2;Y_1|\mathbf{V}_1) + I(\mathbf{V}_1;\mathbf{V}_2) &= I(\mathbf{V}_1,\mathbf{V}_2;Y_1) - [I(\mathbf{V}_1;Y_1) - I(\mathbf{V}_1;\mathbf{V}_2)] \\ &= \log_2 \frac{1+\mathbf{h}^H (K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{h}}{1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}. \end{aligned} \tag{103}$$

Substituting (102) and (103) into (23), we obtain that

$$\begin{aligned} R_2 &\le I(\mathbf{V}_2;Y_2) - I(\mathbf{V}_1;\mathbf{V}_2) - I(\mathbf{V}_2;Y_1|\mathbf{V}_1) \\ &= \log_2 \frac{1+\mathbf{g}^H (K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{g}}{1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}} - \log_2 \frac{1+\mathbf{h}^H (K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{h}}{1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}} \\ &= \log_2 \frac{1+\mathbf{g}^H (K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{g}}{1+\mathbf{h}^H (K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{h}} + \log_2 \frac{1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}{1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}}. \end{aligned} \tag{104}$$

Applying Lemma 2 with bounds (101) and (104), we have the desired result. ■

Proof: (**Equation (40)**) For convenience,we define

$$d(K_{\mathbf{U}_1}, K_{\mathbf{U}_2}) \triangleq \frac{[1+\mathbf{g}^H(K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{g}][1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}]}{[1+\mathbf{h}^H(K_{\mathbf{U}_1}+K_{\mathbf{U}_2})\mathbf{h}][1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}]}$$
$$= \left[1+\frac{\mathbf{g}^H K_{\mathbf{U}_2}\mathbf{g}}{1+\mathbf{g}^H K_{\mathbf{U}_1}\mathbf{g}}\right]\left[1+\frac{\mathbf{h}^H K_{\mathbf{U}_2}\mathbf{h}}{1+\mathbf{h}^H K_{\mathbf{U}_1}\mathbf{h}}\right]^{-1}. \tag{105}$$

Since $\mathbf{c}_2^H(\alpha)\mathbf{c}_2(\alpha)=1$, we substitute (35) into $d(K_{\mathbf{U}_1}, K_{\mathbf{U}_2})$ and obtain

$$d(K_{\mathbf{U}_1}, K_{\mathbf{U}_2}) = \left[1+\frac{(1-\alpha)P\mathbf{g}^H\mathbf{c}_2(\alpha)\mathbf{c}_2^H(\alpha)\mathbf{g}}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\right]\left[1+\frac{(1-\alpha)P\mathbf{h}^H\mathbf{c}_2(\alpha)\mathbf{c}_2^H(\alpha)\mathbf{h}}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\right]^{-1}$$
$$= \frac{\mathbf{c}_2^H(\alpha)\mathbf{c}_2(\alpha)+\dfrac{(1-\alpha)P\mathbf{c}_2^H(\alpha)\mathbf{g}\mathbf{g}^H\mathbf{c}_2(\alpha)}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}}{\mathbf{c}_2^H(\alpha)\mathbf{c}_2(\alpha)+\dfrac{(1-\alpha)P\mathbf{c}_2^H(\alpha)\mathbf{h}\mathbf{h}^H\mathbf{c}_2(\alpha)}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}}$$
$$= \frac{\mathbf{c}_2^H(\alpha)\left[I+\dfrac{(1-\alpha)P\mathbf{g}\mathbf{g}^H}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\right]\mathbf{c}_2(\alpha)}{\mathbf{c}_2^H(\alpha)\left[I+\dfrac{(1-\alpha)P\mathbf{h}\mathbf{h}^H}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\right]\mathbf{c}_2(\alpha)}. \tag{106}$$

Note that $\gamma_2(\alpha)$ and $\mathbf{c}_2(\alpha)$ are the largest generalized eigenvalue and the corresponding normalized eigenvector of the pencil (9), i.e.,

$$\left(I+\frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H\right)\mathbf{c}_2(\alpha) = \gamma_2(\alpha)\left(I+\frac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right)\mathbf{c}_2(\alpha).$$

Hence, we have

$$d_2(K_{\mathbf{U}_1}, K_{\mathbf{U}_2}) = \gamma_2(\alpha). \tag{107}$$

■

APPENDIX IV
SECTION V DERIVATIONS

Proof: (**Lemma 4**) It is sufficient to show that the error probability $P_e^{(n)}$ and the equivocations $H(W_2|Y_1^n)$ and $H(W_2|Y_1^n)$ are the same for the channels $p_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}} \in \mathcal{P}$ when we use the same codebook and encoding schemes. We note that

$$P_e^{(n)} = \max\{P_{e,1}^{(n)}, P_{e,2}^{(n)}\} \leq P_{e,1}^{(n)} + P_{e,2}^{(n)}. \tag{108}$$

Hence, $P_e^{(n)}$ is small if and only if both $P_{e,1}^{(n)}$ and $P_{e,2}^{(n)}$ are small. However, for given codebook and encoding scheme $p(\mathbf{x}^n|w_1,w_2)$, the decoding error probability $P_{e,k}^{(n)}$ and the equivocation rate at user k depend only on the marginal channel probability density $p_{\tilde{Y}_k|\mathbf{X}}$. Therefore, the same code and encoding scheme for any $p_{\tilde{Y}_1,\tilde{Y}_2|\mathbf{X}} \in \mathcal{P}$ gives the same $P_e^{(n)}$ and equivocation rates. This concludes the proof. ■

Proof: (**Theorem 2**) Here we prove Theorem 2 and derive the outer bound for R_1. The outer bound for R_2 follows by symmetry.

The secrecy requirement (7) implies that

$$nR_1 = H(W_1) \leq H(W_1|Y_2^n) + n\epsilon. \tag{109}$$

On the other hand, Fano's inequality and $P_e \leq \epsilon$ imply that

$$H(W_1|Y_1^n) \leq \epsilon \log(M_1 - 1) + h(\epsilon) \triangleq n\delta_1. \tag{110}$$

where $h(x)$ is the binary entropy function. Based on (109) and (110), we have

$$\begin{aligned} nR_1 &\leq H(W_1|Y_2^n) + n\epsilon \\ &\leq H(W_1|Y_2^n) - H(W_1|Y_1^n) + n(\delta_1 + \epsilon) \\ &\leq H(W_1|Y_2^n) - H(W_1|Y_1^n, Y_2^n) + n(\delta_1 + \epsilon) && (111) \\ &= I(W_1; Y_1^n|Y_2^n) + n(\delta_1 + \epsilon) && (112) \end{aligned}$$

where (111) follows from conditioning reducing entropy. Since $W_1 \to \mathbf{X}^n \to (Y_1^n, Y_2^n)$ forms a Markov chain, we can further bound (112) as follows

$$\begin{aligned} nR_1 &\leq I(\mathbf{X}^n; Y_1^n|Y_2^n) + n(\delta_1 + \epsilon) \\ &\leq \sum_{i=1}^{n} I(\mathbf{X}_i; Y_{1,i}|Y_{2,i}) + n(\delta_1 + \epsilon). && (113) \end{aligned}$$

Finally, by applying Lemma 4, we can replace Y_1 and Y_2 by $\tilde{Y}_1$ and $\tilde{Y}_2$, respectively. Hence, we have the Sato-type outer bound on R_1. ■

Proof: (**Lemma 5**) Here, we proof Lemma 5 based on the Sato-type outer bound in Theorem 2.

For the Gaussian BC defined in (45), the upper bound (42) on R_1 can be rewritten as follows:

$$\begin{aligned} I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2)-I(\mathbf{X};\tilde{Y}_2) &= h(\tilde{Y}_1,\tilde{Y}_2)-h(\tilde{Y}_1,\tilde{Y}_2|\mathbf{X})-h(\tilde{Y}_2)+h(\tilde{Y}_2|\mathbf{X}) \\ &= h(\tilde{Y}_1|\tilde{Y}_2)-[h(\tilde{Z}_1,\tilde{Z}_2)-h(\tilde{Z}_2)] \\ &= h(\tilde{Y}_1|\tilde{Y}_2)-\log_2(2\pi e)(1-|\rho|^2). \end{aligned} \tag{114}$$

The first term of (114) can be further bounded as follows

$$\begin{aligned} h(\tilde{Y}_1|\tilde{Y}_2) &= h(\tilde{Y}_1-\nu\tilde{Y}_2|\tilde{Y}_2) \\ &\le h(\tilde{Y}_1-\nu\tilde{Y}_2) \qquad \text{for any } \nu\in\mathbb{C} \end{aligned} \tag{115}$$

where the inequality follows from removing conditioning. Moreover, the maximum-entropy theorem [22] implies that

$$\begin{aligned} h(\tilde{Y}_1-\nu\tilde{Y}_2) &\le \log_2(2\pi e)\big|\mathrm{Var}\big[\tilde{Y}_1-\nu\tilde{Y}_2\big]\big| \\ &= \log_2(2\pi e)\big|\mathrm{Var}\big[(\mathbf{h}-\nu\mathbf{g})^H\mathbf{X}\big]+\mathrm{Var}\big[\tilde{Z}_1-\nu\tilde{Z}_2\big]\big| \\ &= \log_2(2\pi e)\big[(\mathbf{h}-\nu\mathbf{g})^H K_{\mathbf{X}}(\mathbf{h}-\nu\mathbf{g})+1+|\nu|^2-\nu^*\rho-\rho^*\nu\big]. \end{aligned} \tag{116}$$

Combining (114), (115) and (116), we obtain the following upper bound:

$$I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2)-I(\mathbf{X};\tilde{Y}_2) \le \min_{\nu\in\mathbb{C}} \log_2 \frac{(\mathbf{h}-\nu\mathbf{g})^H K_{\mathbf{X}}(\mathbf{h}-\nu\mathbf{g})+1+|\nu|^2-\nu^*\rho-\rho^*\nu}{(1-|\rho|^2)} \tag{117}$$

$$= f_1(\rho, K_{\mathbf{X}}). \tag{118}$$

Next we prove that for given ρ and $K_{\mathbf{X}}$, the expression $I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2)-I(\mathbf{X};\tilde{Y}_2)$ is maximized by Gaussian input distributions. When $\mathbf{X}$ is a Gaussian random vector with zero-mean and covariance matrix $K_{\mathbf{X}}$, the channel (45) implies that $\tilde{Y}_1$ and $\tilde{Y}_2$ are zero-mean Gaussian random variables. Choosing

$$\nu=\nu_{\mathrm{o}}=\frac{\mathrm{Cov}\big[\tilde{Y}_1,\tilde{Y}_2\big]}{\mathrm{Var}\big[\tilde{Y}_2\big]}. \tag{119}$$

Note that

$$\mathrm{E}\big[(\tilde{Y}_1-\nu_{\mathrm{o}}\tilde{Y}_2)\tilde{Y}_2^*\big]=\mathrm{Cov}\big[\tilde{Y}_1,\tilde{Y}_2\big]-\nu_{\mathrm{o}}\mathrm{Var}\big[\tilde{Y}_2\big]=0, \tag{120}$$

the Gaussian random variables $\tilde{Y}_1-\nu_{\mathrm{o}}\tilde{Y}_2$ and $\tilde{Y}_2$ are uncorrelated, and hence they are statistically inde-

pendent. This implies that

$$\begin{aligned} h(\tilde{Y}_1|\tilde{Y}_2) &= h(\tilde{Y}_1 - \nu_{\rm o}\tilde{Y}_2) \\ &= \log_2(2\pi e)\big[(\mathbf{h}-\nu_{\rm o}\mathbf{g})^H K_{\mathbf{X}}(\mathbf{h}-\nu_{\rm o}\mathbf{g}) + 1 + |\nu_{\rm o}|^2 - \nu_{\rm o}^*\rho - \rho^*\nu_{\rm o}\big]. \end{aligned} \tag{121}$$

Inserting (121) into (114) we have

$$\begin{aligned} I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2) - I(\mathbf{X};\tilde{Y}_2) &= \log_2 \frac{(\mathbf{h}-\nu_{\rm o}\mathbf{g})^H K_{\mathbf{X}}(\mathbf{h}-\nu_{\rm o}\mathbf{g}) + 1 + |\nu_{\rm o}|^2 - \nu_{\rm o}^*\rho - \rho^*\nu_{\rm o}}{(1-|\rho|^2)} \\ &\geq f_1(\rho, K_{\mathbf{X}}). \end{aligned} \tag{122}$$

Bounds (118) and (122) imply that Gaussian input distributions are optimal for the expression $I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2) - I(\mathbf{X};\tilde{Y}_2)$.

Following the same approach, we can prove that for given ρ and $K_{\mathbf{X}}$, Gaussian input distributions maximize the expression $I(\mathbf{X};\tilde{Y}_1,\tilde{Y}_2) - I(\mathbf{X};\tilde{Y}_1)$, the upper bound (43) on R_2. This lets us restrict attention to zero-mean Gaussian $\mathbf{X}$ with covariance matrix $K_{\mathbf{X}}$. Now, bounds (42) and (43) become

$$R_1 \leq f_1(\rho, K_{\mathbf{X}}) \tag{123}$$

and

$$R_2 \leq f_2(\rho, K_{\mathbf{X}}) \tag{124}$$

This yields the rate region $\mathcal{R}_{\rm O}^{\rm MG}(\rho, K_{\mathbf{X}})$. Hence we have the desired result. ∎

Proof: (**Lemma 6**) For a given $K_{\mathbf{X}}$, we first evaluate $L(K_{\mathbf{X}}, 0)$ and $L(K_{\mathbf{X}}, 1)$. Since $\gamma_1(0) = 1$ and the input covariance matrix $K_{\mathbf{X}}$ is positive semidefinite, we obtain

$$L(K_{\mathbf{X}}, 0) = (\mathbf{h}-\rho_{\rm o}\mathbf{g})^H K_{\mathbf{X}}(\mathbf{h}-\rho_{\rm o}\mathbf{g}) \geq 0. \tag{125}$$

On the other hand, since $\gamma_1(1) = \lambda_1$ and $K_{\mathbf{X}}$ is Hermitian and positive semidefinite, we have

$$\begin{aligned} L(K_{\mathbf{X}}, 1) &= (\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g})^H (K_{\mathbf{X}} - P\mathbf{e}_1\mathbf{e}_1^H)(\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g}) \\ &\leq \operatorname{tr}(K_{\mathbf{X}})|\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g}|^2 - P|(\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g})^H\mathbf{e}_1|^2 \\ &\leq P|\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g}|^2 - P|(\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g})^H\mathbf{e}_1|^2. \end{aligned} \tag{126}$$

Based on the definition of $\rho_{\rm o}$ in (51), we can compute

$$\begin{aligned}\mathbf{h}-\rho_{\rm o}\lambda_1\mathbf{g} &= \mathbf{h}-\lambda_1\frac{\mathbf{g}\mathbf{g}^H\mathbf{e}_1}{\mathbf{h}^H\mathbf{e}_1}\\ &= \frac{(\mathbf{h}\mathbf{h}^H-\lambda_1\mathbf{g}\mathbf{g}^H)\mathbf{e}_1}{\mathbf{h}^H\mathbf{e}_1}\\ &= \frac{(\lambda_1-1)\mathbf{e}_1}{P\mathbf{h}^H\mathbf{e}_1}\end{aligned} \tag{127}$$

where the last step follows from the definitions λ_1 and $\mathbf{e}_1$ in (2). Moreover, since $\mathbf{e}_1^H\mathbf{e}_1 = 1$, (127) can be rewritten as

$$\begin{aligned}L(K_{\mathbf{X}},1) &\le P\left|\frac{(\lambda_1-1)\mathbf{e}_1}{P\mathbf{h}^H\mathbf{e}_1}\right|^2 - P\left|\frac{\lambda_1-1}{P\mathbf{h}^H\mathbf{e}_1}\mathbf{e}_1^H\mathbf{e}_1\right|^2\\ &= 0\end{aligned} \tag{128}$$

We note that $L(K_{\mathbf{X}},\alpha)$ is a continuous function on the interval $\alpha\in[0,1]$ for a give $K_{\mathbf{X}}$. Since $L(K_{\mathbf{X}},0)\ge 0$ and $L(K_{\mathbf{X}},1)\le 0$, there exists $\alpha\in[0,1]$ such that $L(K_{\mathbf{X}},\alpha)=0$. ■

Proof: (**Lemma 7**) We note that λ_1 and $\mathbf{e}_1$ are the largest generalized eigenvalue and the corresponding normalized eigenvector of the pencil $[I+P\mathbf{h}\mathbf{h}^H, I+P\mathbf{g}\mathbf{g}^H]$. Based on the Rayleigh's quotient principle in Theorem 3, we obtain

$$\max_{\mathbf{c}}\frac{\mathbf{c}^H(I+P\mathbf{h}\mathbf{h}^H)\mathbf{c}}{\mathbf{c}^H(I+P\mathbf{g}\mathbf{g}^H)\mathbf{c}} = \frac{\mathbf{e}_1^H(I+P\mathbf{h}\mathbf{h}^H)\mathbf{e}_1}{\mathbf{e}_1^H(I+P\mathbf{g}\mathbf{g}^H)\mathbf{e}_1} = \lambda_1. \tag{129}$$

Hence, we have

$$\min_{\mathbf{c}}\frac{(1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2)+\mathbf{c}^H[(1-\alpha)P\mathbf{g}\mathbf{g}^H]\mathbf{c}}{(1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2)+\mathbf{c}^H[(1-\alpha)P\mathbf{h}\mathbf{h}^H]\mathbf{c}} = \frac{\mathbf{e}_1^H(I+P\mathbf{g}\mathbf{g}^H)\mathbf{e}_1}{\mathbf{e}_1^H(I+P\mathbf{h}\mathbf{h}^H)\mathbf{e}_1} = \frac{1}{\lambda_1}. \tag{130}$$

By using the definition of $\gamma_1(\alpha)$ in (8), we have

$$\min_{\mathbf{c}}\frac{\mathbf{c}^H\left[I+\dfrac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H\right]\mathbf{c}}{\mathbf{c}^H\left[I+\dfrac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right]\mathbf{c}} = \frac{\mathbf{e}_1^H\left[I+\dfrac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H\right]\mathbf{e}_1}{\mathbf{e}_1^H\left[I+\dfrac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right]\mathbf{e}_1} = \frac{\gamma_1(\alpha)}{\lambda_1}. \tag{131}$$

Now, the Rayleigh's quotient principle implies that $\gamma_1(\alpha)/\lambda_1$ and $\mathbf{e}_1(\alpha)$ are the smallest generalized eigenvalue and the corresponding normalized eigenvector of the pencil (9). ■

Proof: (**Lemma 8**) We first show that $[\mathbf{g} - \rho_{\mathrm{o}}^* \gamma_2(\alpha)\mathbf{h}] \propto \mathbf{c}_2(\alpha)$. Since $\gamma_1(\alpha)$ is real and

$$\rho_{\mathrm{o}} = \frac{1}{\gamma_1(\alpha)} \left[\frac{\mathbf{h}^H \mathbf{c}_2(\alpha)}{\mathbf{g}^H \mathbf{c}_2(\alpha)}\right]^*, \tag{132}$$

we have

$$\begin{aligned}\mathbf{g} - \rho_{\mathrm{o}}^* \gamma_2(\alpha)\mathbf{h} &= \mathbf{g} - \frac{\gamma_2(\alpha)}{\gamma_1(\alpha)} \frac{\mathbf{h}\mathbf{h}^H \mathbf{c}_2(\alpha)}{\mathbf{g}^H \mathbf{c}_2(\alpha)} \\ &= \frac{[\gamma_1(\alpha)\mathbf{g}\mathbf{g}^H - \gamma_2(\alpha)\mathbf{h}\mathbf{h}^H]\mathbf{c}_2(\alpha)}{\gamma_1(\alpha)\mathbf{g}^H \mathbf{c}_2(\alpha)}.\end{aligned} \tag{133}$$

Note that (36) implies that

$$\left[\frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H \mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H - \gamma_2(\alpha)\frac{(1-\alpha)P}{1+\alpha P|\mathbf{h}^H \mathbf{e}_1|^2}\mathbf{h}\mathbf{h}^H\right]\mathbf{c}_2(\alpha) = [\gamma_2(\alpha) - 1]\mathbf{c}_2(\alpha). \tag{134}$$

Based on the definition of $\gamma_1(\alpha)$ in (8), we obtain

$$[\gamma_1(\alpha)\mathbf{g}\mathbf{g}^H - \gamma_2(\alpha)\mathbf{h}\mathbf{h}^H]\mathbf{c}_2(\alpha) = \frac{1+\alpha P|\mathbf{h}^H \mathbf{e}_1|^2}{(1-\alpha)P}[\gamma_2(\alpha) - 1]\mathbf{c}_2(\alpha). \tag{135}$$

Now, we can rewritten (133) as

$$\mathbf{g} - \rho_{\mathrm{o}}^* \gamma_2(\alpha)\mathbf{h} = \frac{(1+\alpha P|\mathbf{h}^H \mathbf{e}_1|^2)[\gamma_2(\alpha) - 1]}{\gamma_1(\alpha)\mathbf{g}^H \mathbf{c}_2(\alpha)(1-\alpha)P}\mathbf{c}_2(\alpha). \tag{136}$$

Hence, we obtain

$$\frac{\mathbf{g} - \rho_{\mathrm{o}}^* \gamma_2(\alpha)\mathbf{h}}{|\mathbf{g} - \rho_{\mathrm{o}}^* \gamma_2(\alpha)\mathbf{h}|^2} = \mathbf{c}_2(\alpha). \tag{137}$$

Next we prove that $[\mathbf{h} - \rho_{\mathrm{o}} \gamma_1(\alpha)\mathbf{g}]^H \mathbf{c}_2(\alpha) = 0$. The definitions of λ_1 and $\mathbf{e}_1$ in (2) implies that

$$\mathbf{h}\mathbf{h}^H \mathbf{e}_1 = \left[\frac{\lambda_1 - 1}{P} I + \lambda_1 \mathbf{g}\mathbf{g}^H\right]\mathbf{e}_1. \tag{138}$$

Substituting (138) into (59), we obtain

$$\begin{aligned}\mathbf{h} - \rho_{\mathrm{o}} \gamma_1(\alpha)\mathbf{g} &= \frac{1}{\mathbf{h}^H \mathbf{e}_1}\left[\frac{\lambda_1 - 1}{P} I + \lambda_1 \mathbf{g}\mathbf{g}^H - \gamma_1(\alpha)\mathbf{g}\mathbf{g}^H\right]\mathbf{e}_1 \\ &= \frac{\lambda_1 - 1}{P\mathbf{h}^H \mathbf{e}_1}\left[I + \frac{\lambda_1 - \gamma_1(\alpha)}{\lambda_1 - 1} P\mathbf{g}\mathbf{g}^H\right]\mathbf{e}_1.\end{aligned} \tag{139}$$

Based on the definition of $\gamma_1(\alpha)$ in (8), we obtain

$$\begin{aligned}\lambda_1 - \gamma_1(\alpha) &= \lambda_1 - \frac{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2} \\ &= \frac{(\lambda_1 - 1) + \alpha P(\lambda_1|\mathbf{g}^H\mathbf{e}_1|^2 - |\mathbf{h}^H\mathbf{e}_1|^2)}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2} \\ &= (\lambda_1 - 1)\frac{1-\alpha}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\end{aligned} \tag{140}$$

where the last step follows from (52). Substituting (139) into (140), we have

$$\mathbf{h} - \rho_o\gamma_1(\alpha)\mathbf{g} = \frac{\lambda_1 - 1}{P\mathbf{h}^H\mathbf{e}_1}\left[I + \frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\mathbf{g}\mathbf{g}^H\right]\mathbf{e}_1. \tag{141}$$

Now (64) and (141) imply that

$$[\mathbf{h} - \rho_o\gamma_1(\alpha)\mathbf{g}]^H\mathbf{c}_2(\alpha) = 0. \tag{142}$$

Combining with (137), we have the desired result. ■

Proof: (**Equation (77)**) First, we consider $\zeta(\alpha)$ defined in (75). Based on (133) and (136), $\zeta(\alpha)$ can be rewritten as

$$\begin{aligned}\zeta(\alpha) &= [\mathbf{g} - \rho_o^*\gamma_2(\alpha)\mathbf{h}]^H[\mathbf{g} - \rho_o^*\gamma_2(\alpha)\mathbf{h}] \\ &= \frac{(1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2)[\gamma_2(\alpha) - 1]}{(1-\alpha)P}\left\{\frac{\mathbf{c}_2^H(\alpha)[\gamma_1(\alpha)\mathbf{g}\mathbf{g}^H - \gamma_2(\alpha)\mathbf{h}\mathbf{h}^H]\mathbf{c}_2(\alpha)}{|\gamma_1(\alpha)\mathbf{g}^H\mathbf{c}_2(\alpha)|^2}\right\} \\ &= \left[\frac{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}{(1-\alpha)P}\right][\gamma_2(\alpha) - 1]\left[\frac{1}{\gamma_1(\alpha)} - \gamma_2(\alpha)|\rho_o|^2\right].\end{aligned} \tag{143}$$

Now, we consider

$$\begin{aligned}(1-\alpha)P\zeta(\alpha) &= [\gamma_2(\alpha) - 1][1 + \alpha P|\mathbf{g}^H\mathbf{e}_1|^2 - \gamma_2(\alpha)|\rho_o|^2 - \alpha P|\mathbf{h}^H\mathbf{e}_1|^2\gamma_2(\alpha)|\rho_o|^2] \\ &= [\gamma_2(\alpha) - 1]\{1 - \gamma_2(\alpha)|\rho_o|^2 + \alpha P|\mathbf{g}^H\mathbf{e}_1|^2[1 - \gamma_2(\alpha)]\}\end{aligned} \tag{144}$$

where the last step of (144) follows from $\rho_o = (\mathbf{g}^H\mathbf{e}_1)/(\mathbf{h}^H\mathbf{e}_1)$.

Next, we consider $\eta(\alpha)$ defined in (76). Note that (66) implies that

$$|\mathbf{e}_1^H\mathbf{c}_2(\alpha)|^2 = \left[\frac{(1-\alpha)P}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2}\right]^2|\mathbf{g}^H\mathbf{e}_1|^2|\mathbf{g}^H\mathbf{c}_2(\alpha)|^2. \tag{145}$$

Combining (132), (143) and (145), we obtain

$$\begin{aligned}\eta(\alpha) &= \zeta(\alpha)|\mathbf{e}_1^H\mathbf{c}_2(\alpha)|^2 \\ &= \frac{(1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2)(\gamma_2(\alpha)-1)}{(1-\alpha)P}\left[\frac{1}{\gamma_1(\alpha)} - \frac{\gamma_2(\alpha)}{\gamma_1^2(\alpha)}\left|\frac{\mathbf{h}^H\mathbf{c}_2}{\mathbf{g}^H\mathbf{c}_2}\right|^2\right]|\mathbf{e}_1^H\mathbf{c}_2(\alpha)|^2 \\ &= [\gamma_2(\alpha)-1]|\mathbf{g}^H\mathbf{e}_1|^2\left[\frac{(1-\alpha)P|\mathbf{g}^H\mathbf{c}_2(\alpha)|^2}{1+\alpha P|\mathbf{g}^H\mathbf{e}_1|^2} - \gamma_2(\alpha)\frac{(1-\alpha)P|\mathbf{h}^H\mathbf{c}_2(\alpha)|^2}{1+\alpha P|\mathbf{h}^H\mathbf{e}_1|^2}\right] \\ &= [\gamma_2(\alpha)-1]^2|\mathbf{g}^H\mathbf{e}_1|^2 \end{aligned} \tag{146}$$

where the last step of (146) follows from the definition of $\gamma_2(\alpha)$ in (36). Combining (144) and (146), we obtain the desired result. ■

REFERENCES

[1] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–138, Oct. 1975.

[2] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inf. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.

[3] Y. Oohama, "Coding for relay channels with confidential messages," in *Proc. IEEE Information Theory Workshop*, Cairns, Australia, Sep. 2001, pp. 87–89.

[4] I. Csiszár and P. Narayan, "Secrecy capacities for multiple terminal," *IEEE Trans. Inf. Theory*, vol. 50, no. 12, pp. 3047–3061, Dec 2004.

[5] E. Tekin and A. Yener, "The Gaussian multiple access wire-tap channel with collective secrecy constraints," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, USA, Jul. 2006.

[6] ——, "The multiple access wire-tap channel: Wireless secrecy and cooperative jamming," in *Proc. Information Theory and Application Workshop, ITA*, San Diego, CA, Jan. 2007.

[7] Y. Liang and H. Vincent Poor, "Generalized multiple access channels with confidential messages," *IEEE Trans. Inf. Theory*, submitted (under revision), April 2006. [Online]. Available: http://arxiv.org/PS$_$cache/cs/pdf/0605/0605014.pdf

[8] R. Liu, I. Maric, R. D. Yates, and P. Spasojevic, "The discrete memoryless multiple access channel with confidential messages," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Jul. 2006, pp. 957 – 961.

[9] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages," in *Proc. Allerton Conference on Communication, Control, and Computing*, Sep. 2006.

[10] L. Lai and H. El Gamal, "The relay-eavesdropper channel: Cooperation for secrecy," *IEEE Trans. Inf. Theory*, submitted, Dec. 2006.

[11] M. Yuksel and E. Erkip., "The relay channel with a wiretapper," in *Proc. Forty-First Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, Mar. 2007.

[12] J. Barros and M. Rodrigues, "Secrecy capacity of wireless channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Seattle, USA, Jul. 2006.

[13] Z. Li, R. Yates, and W. Trappe, "Secrecy capacity of indepedent parallel channels," in *Proc. Allerton Conference on Commun., Contr., Computing*, Monticello, IL, USA, Sep. 2006.

[14] Y. Liang, H. Vincent Poor, and S. Shamai (Shitz), "Secure communication over fading channels," *IEEE Trans. Inf. Theory*, submitted, Nov. 2006. [Online]. Available: http://arxiv.org/PS$_$cache/cs/pdf/0701/0701024.pdf

[15] P. Gopala, L. Lai, and H. El Gamal, "On the secrecy capacity of fading channels," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007.

[16] Z. Li, W. Trappe, and R. Yates, "Secret communication via multi-antenna transmission," in *Proc. Forty-First Annual Conference on Information Sciences and Systems (CISS)*, Baltimore, MD, USA, Mar. 2007.

[17] R. Liu and H. Vincent Poor, "Multiple antenna secure broadcast over wireless networks," in *Proc. First International Workshop on Information Theory for Sensor Networks*, Santa Fe, NM, June 18-20, 2007, pp. 125–139.

[18] A. Khisti, G. Wornell, A. Wiesel, and Y. Eldar, "On the Gaussian MIMO wiretap channel," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007.

[19] A. Khisti and G. Wornell, "Secure transmission with multiple antennas: The MISOME wiretap channel," *IEEE Trans. Inf. Theory*, submitted, August 2007.

[20] S. Shafiee and S. Ulukus, "Achievable rates in gaussian MISO channels with secrecy constraints," in *Proc. IEEE Int. Symp. Information Theory (ISIT)*, Nice, France, June 24-29, 2007.

[21] S. Shafiee, N. Liu, and S. Ulukus, "Towards the secrecy capacity of the Gaussian MIMO wire-tap channel: The 2-2-1 channel," *IEEE Trans. Inf. Theory*, submitted, September 2007.

[22] T. Cover and J. Thomas, *Elements of Information Theory*. New York: John Wiley Sons, Inc., 1991.

[23] S. K. Leung-Yan-Cheong and M. E. Hellman, "The Gaussian wire-tap channel," *IEEE Trans. Inf. Theory*, vol. 24, no. 4, pp. 51–456, Jul. 1978.

[24] R. Liu, I. Maric, P. Spasojevic, and R. Yates, "Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions," *IEEE Trans. Inf. Theory*, submitted, Feb 2007. [Online]. Available: http://arxiv.org/PS$_$cache/cs/pdf/0702/0702099.pdf

[25] U. Maurer and S. Wolf, "Information-theoretic key agreement: From weak to strong secrecy for free," in *Proc. EUROCRYPT, Lecture Notes in Computer Science*, vol. 1807, 2000, pp. 351–368.

[26] D. Slepian and J. K. Wolf, "Noiseless coding of correlated information sources," *IEEE Trans. Inf. Theory*, vol. 19, no. 4, pp. 471–480, Jul. 1973.

[27] K. Marton, "A coding theorem for the discrete memoryless broadcast channel," *IEEE Trans. Inf. Theory*, vol. 25, pp. 306–311, May 1979.

[28] G. Caire and S. Shamai (Shitz), "On the achievable throughput of a multiantenna Gaussian broadcast channel," *IEEE Trans. Inf. Theory*, vol. 49, no. 7, pp. 1691–1706, Jul. 2003.

[29] W. Yu and J. M. Cioffi, "Sum capacity of Gaussian vector broadcast channels," *IEEE Trans. Inf. Theory*, vol. 50, pp. 1875–1892, Sep. 2004.

[30] G. Strang, *Linear Algebra and Its Applications*. Wellesley, MA: Wellesley-Cambridge Press, 1998.